#4

Express Mail No.: EL211266044US

IN THE UNITED STATES PATENT AND PATENT
TRADEMARK OFFICE

PETITION UNDER C.F.R. 1.181

Applicant(s):	Osamu SHIBATA, et al.	Docket No.:	29288.0300
Serial No.:	09/828,559	Filed:	April 6, 2001
TITLE:	COPYRIGHT PROTECTION SYSTEM, ENCRYPTION DEVICE, DECRYPTION DEVICE, AND RECORDING MEDIUM	Group Art Unit:	TBA

Commissioner for Patents
Box **PETITIONS**
Washington, D.C. 20231-9998

Sir:

Applicant, pursuant to 37 CFR §1.181, hereby petitions to proceed with prosecution of the above-referenced patent application which was misplaced due to an error by the U.S. Patent and Trademark Office.

On April 6, 2001, the undersigned filed the attached Patent Application 37 C.F.R. 1.53(b) and received a return postcard with the Serial Number 09/828,559 stamped thereon by the USPTO office and confirming receipt of same on April 6, 2001.

On March 3, 2003, the undersigned prepared to file an Information Disclosure Statement in the above-referenced matter, at which time it was discovered that there was no Filing Receipt in the file, nor had we received a Notice to File Missing Parts as a signed declaration was not available at the time this application was filed. A member of my staff contacted the U.S. Patent and Trademark Office's Office of Initial Patent Examination (OIPE) to determine why we had not received an Official Filing Receipt or Notice to File Missing Parts and was informed by a clerk of that office that our Customer Number had been incorrectly entered into your tracking system and thus our documents were sent to another firm who did not act upon them and the application was abandoned for failure to respond. He then stated he would retrieve the file and rectify the situation.

After several weeks, my assistant again contacted the OIPE, and spoke with Monica Young who confirmed the error in the Customer Number but indicated it looked like our previous request had not been acted upon.

Ms. Young then informed my assistant that she would retrieve the file from the repository and proceed to have the case reinstated as the error was obviously a USPTO error. Ms. Young stated she would contact my assistant once the file was returned from the repository but to be patient as it could take some time.

After several weeks, my assistant attempted to contact Ms. Young several times and once able to reach her was informed that the USPTO's system showed the file should be in her area but that it had not yet made it to her desk. Ms. Young did indicate that the file showed in the system as having been in her area for several days and that it was strange it had not yet made it to her desk. She then indicated she would initiate a search for the file and contact my assistant once it was located. It has again been several weeks since my assistant has heard from Ms. Young. She has made attempts to contact her in the last few days, but has yet to receive a response.

It was then determined that we submit this Petition and request that prosecution proceed.

Therefore, please treat the attached paperwork as if it is the original application which was filed on April 6, 2001, by this office and grant the application that filing date. We also hereby revoke any instructions to charge the filing fees to our Deposit Account No. 19-2814 with regard to this application as the filing fee was already submitted in the form of Check No. 501019, a copy of which is enclosed.

Should the Commissioner or his Examiner wish to discuss this matter, please contact the undersigned at (602) 382-6377.

Respectfully submitted,

By____________________ 8/12/03
Michael K. Kelly
Reg. No. 32,848

SNELL & WILMER L.L.P.
One Arizona Center
400 East Van Buren
Phoenix, Arizona 85004-2202
(602) 382-6377

#14

Snell & Wilmer
L.L.P.
LAW OFFICES

One Arizona Center
Phoenix, Arizona 85004-2202
(602) 382-6000
Fax: (602) 382-6070
www.swlaw.com

PHOENIX, ARIZONA
TUCSON, ARIZONA
IRVINE, CALIFORNIA
SALT LAKE CITY, UTAH
DENVER, COLORADO
LAS VEGAS, NEVADA

FACSIMILE TRANSMISSION

DATE: November 17, 2003

TIME IN: 1 35 AP
TIME OUT:

TO:

Name	Fax Number	Phone Number
Cliff Congo Office of Petitions - USPTO	**703-308-6916**	703-305-0272

FROM: Julie Eslick PHONE: 602-382-6854

RE: U.S. Serial No. 09/828,559 - Petition Under CFR 1.181

MESSAGE:

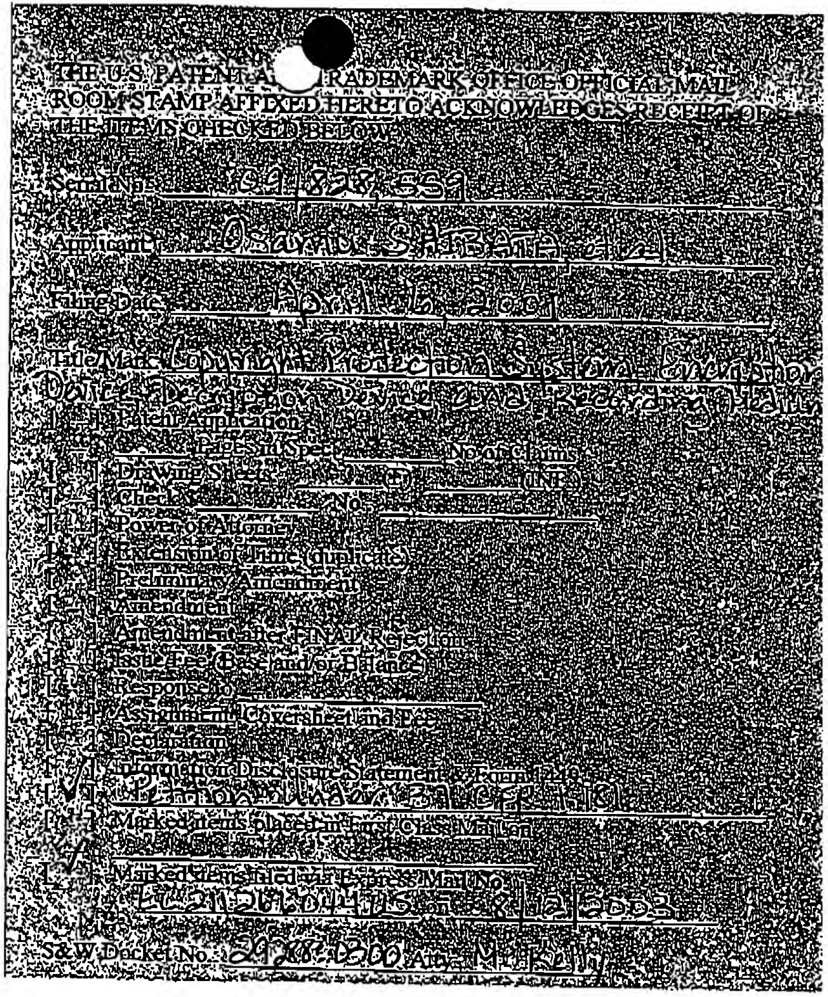
Cliff:

Per our conversation, attached is a copy of our petition which was filed on August 12, 2003. If you need anything further, please do not hesitate to contact me. Please confirm receipt of this transmission by return facsimile. Thanks.
Julie A. Eslick
Patent & Trademark Assistant

ORIGINAL DOCUMENT:	Will not be sent	NUMBER OF PAGES (Including Cover):	77
CONFIRMATION NO.:		CLIENT MATTER NO.:	29288.0300
PLEASE RETURN TO:	Julie Eslick at 16I07	PERSONAL FAX:	No
REQUESTOR:	Julie Eslick	DIRECT LINE:	602-382-6854

**IF YOU HAVE NOT PROPERLY RECEIVED THIS TELECOPY, PLEASE CALL US AT (602) 382-6075.
OUR FACSIMILE NUMBER IS (602) 382-6070.**

THE INFORMATION CONTAINED IN THIS FACSIMILE MESSAGE IS ATTORNEY PRIVILEGED AND CONFIDENTIAL INFORMATION INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY NAMED ABOVE. IF THE READER OF THIS MESSAGE IS NOT THE INTENDED RECIPIENT, OR THE EMPLOYEE OR AGENT RESPONSIBLE TO DELIVER IT TO THE INTENDED RECIPIENT, YOU ARE HEREBY NOTIFIED THAT ANY DISSEMINATION, DISTRIBUTION OR COPYING OF THIS COMMUNICATION IS STRICTLY PROHIBITED. IF YOU HAVE RECEIVED THIS COMMUNICATION IN ERROR, PLEASE IMMEDIATELY NOTIFY US BY TELEPHONE, AND RETURN THE ORIGINAL MESSAGE TO US AT THE ABOVE ADDRESS VIA THE U.S. POSTAL SERVICE. THANK YOU.



Serial No.: 09/828,559

Applicant: Osamu SHIBATA et al

Filing Date: April 6, 2001

Title/Mat.: Copyright Protection System, Encryption Device, Decryption Device and Recording Mediu

[ ] Patent Application
 Pages in Spec. No. of Claims
[ ] Drawing Sheets (F) (INF)
[ ] Check No.
[ ] Power of Attorney
[ ] Extension of Time (duplicate)
[ ] Preliminary Amendment
[ ] Amendment
[ ] Amendment after FINAL Rejection
[ ] Issue Fee (Base and/or Balance)
[ ] Response to
[ ] Assignment, Coversheet and Fee
[ ] Declaration
[✓] Information Disclosure Statement & Form 1449
[✓] Petition Under 37 CFR 1.181
[ ] Marked items placed in First Class Mail on
[illegible]
[✓] Marked items filed via Express Mail No.
EL211260441US on 8/12/2003

S&W Docket No. 29288-0300 Atty. M. Kelly [redacted] EL211266044US

EXPRESS MAIL
UNITED STATES POSTAL SERVICE™

EL211266044US

POST OFFICE TO ADDRESSEE

Mailing Label
Label 11-F July 1997

ORIGIN (POSTAL USE ONLY)

PO ZIP Code	Day of Delivery □ Next □ Second	Flat Rate Envelope □
Date In Mo. Day Year	□ 12 Noon □ 3 PM	Postage $
Time In □ AM □ PM	Military □ 2nd Day □ 3rd Day	Return Receipt Fee
Weight lbs. ozs.	Int'l Alpha Country Code	COD Fee / Insurance Fee
No Delivery □ Weekend □ Holiday	Acceptance Clerk Initials	Total Postage & Fees $

DELIVERY (POSTAL USE ONLY)

Delivery Attempt Mo. Day	Time □ AM □ PM	Employee Signature
Delivery Attempt Mo. Day	Time □ AM □ PM	Employee Signature
Delivery Date Mo. Day	Time □ AM □ PM	Employee Signature

Signature of Addressee or Agent
X

Name - Please Print
X

CUSTOMER USE ONLY
METHOD OF PAYMENT:
Express Mail Corporate Acct. No. X852770
Federal Agency Acct. No. or Postal Service Acct. No.

□ WAIVER OF SIGNATURE (Domestic Only): Additional merchandise insurance is void if waiver of signature is requested. I wish delivery to be made without obtaining signature of addressee or addressee's agent (if delivery employee judges that article can be left in secure location) and I authorize that delivery employee's signature constitutes valid proof of delivery.
NO DELIVERY □ Weekend □ Holiday
Customer Signature

744/ 10
F02
T

FROM: (PLEASE PRINT) PHONE

ATTORNEY: Michael K. Kelly
FILE # 29788.0300 DATE 8/12/2003
SNELL & WILMER LLP
400 E VAN BUREN ST
1 ARIZONA CENTER
PHOENIX AZ 85004-2223

TO: (PLEASE PRINT) PHONE ( )

COMMISSIONER FOR PATENTS
MAIL STOP PETITIONS
PO BOX 1450
ALEXANDRIA, VA 22313-1450

PRESS HARD.
You are making 3 copies.

FOR PICKUP OR TRACKING CALL 1-800-222-1811 www.usps.gov EMS

2112604

THE U.S. PATENT AND TRADEMARK OFFICE OFFICIAL MAIL ROOM STAMP AFFIXED HERETO ACKNOWLEDGES RECEIPT OF THE ITEMS CHECKED BELOW:

Serial No. To be Assigned

Applicant: Osamu SHIBATA, et al.

Filing Date: April 6, 2001

Title/Mark: Copyright Protection System, Encryption Device, Decryption Device, and Recording Medium

[✓] Patent Application

✓ 51 Pages in Spec 47 No. of Claims

[✓] Drawing Sheets 9 (F) ___ (INF.)

[✓] Check $ 1276.00 No. ______

[ ] Power of Attorney

[ ] Extension of Time (duplicate)

[ ] Preliminary Amendment

THE U.S. PATENT AND TRADEMARK OFFICE OFFICIAL MAIL ROOM STAMP AFFIXED HERETO ACKNOWLEDGES RECEIPT OF THE ITEMS CHECKED BELOW:

Serial No. To be Assigned

Applicant: Osamu SHIBATA, et al.

Filing Date: April 6, 2001

Title/Mark: Copyright Protection System, Encryption Device, Decryption Device, and Recording Medium

[✓] Patent Application

✓ 51 Pages in Spec 47 No. of Claims

[✓] Drawing Sheets 9 (F) ___ (INF.)

[✓] Check $ 1276.00 No. ______

[ ] Power of Attorney

[ ] Extension of Time (duplicate)

[ ] Preliminary Amendment

[ ] Amendment

[ ] Amendment after FINAL Rejection

[ ] Issue Fee (Base and/or Balance)

[ ] Small Entity Certificate

[ ] Assignment, Cover Sheet and Fee

[ ] Trademark Application

[✓] Priority Document 2000-105535

[✓] IDS w/ PTO-1449 and References

[ ] Mailed item placed in First Class Mail on

[✓] Mailed item sent via Express Mail No. EL339435647US - April 6, 2001

Atty Docket No. [redacted] Atty. H. Kelly

41133-0200

SNELL & WILMER
One Arizona Center
400 E. Van Buren
Phoenix

Attn: Intellectual Property Dept.

NOTED ON DOCKET/K. WRIGHT

EM339435647US

POST OFFICE TO ADDRESSEE

EXPRESS MAIL
UNITED STATES POSTAL SERVICE

EMS

EM339435647US

ORIGIN (POSTAL USE ONLY)

INTERNATIONAL SHIPMENTS ONLY
□ Business Papers
□ Merchandise
Customs forms and commercial invoice may be required. See Pub 273 and International Mail Manual.

PO ZIP 85034

Day of Delivery ☒ Next □ Second

□ Flat Rate Envelope

Date In 4 6 01

☒ 12 Noon □ 3 PM

Postage $ 16 00

Time In 413 □ AM ☒ PM

Military □ 2nd Day □ 3rd Day

Return Receipt

Weight 1 lbs 4 oz

Int'l Alpha Country Code

C.O.D.

No Delivery □ Weekend □ Holiday

Acceptance Clerk Initials B

Total Postage & Fees $ 16 00

SEE REVERSE SIDE FOR THE SERVICE GUARANTEE AND LIMITS ON THE INSURANCE COVERAGE

CUSTOMER USE ONLY

METHOD OF PAYMENT:
Express Mail Corporate Acct. No. X852770
Federal Agency Acct. No. or Postal Service Acct. No.

□ WAIVER OF SIGNATURE (Domestic Only) [illegible]

NO DELIVERY □ WEEKEND □ HOLIDAY

FROM: (PLEASE PRINT) PHONE

ATTORNEY: Michael K. Kelly
FILE # 29288.0300 DATE 4/6/01
SNELL & WILMER LLP
400 E VAN BUREN ST
1 ARIZONA CENTER
PHOENIX AZ 85004-2223

TO: (PLEASE PRINT) PHONE

BOX New Application
ASSISTANT COMMISSIONER FOR
PATENTS
WASHINGTON DC 20231-0001

EM339435647US

SNELL & WILMER - PHOENIX, ARIZONA L.L.P. 501019

INVOICE NO	DATE	DESCRIPTION	INVOICE AMOUNT	DISCOUNT	NET AMOUNT
040501D	04/05/01	JULIE E 28569-0001	1276.00	0.00	1276.00
VEND: 1755		501019	1276.00	0.00	1276.00

SNELL & WILMER
L.L.P.
ONE ARIZONA CENTER
PHOENIX, ARIZONA 85004-0001

WITH OFFICES IN:
TUCSON, ARIZONA
IRVINE, CALIFORNIA
SALT LAKE CITY, UTAH

BANK ONE, ARIZONA, NA
P.O. BOX 71, PHOENIX, ARIZONA 85001

91-2/1221

CHECK NO. 501019

	DATE	CHECK NO.
VEND: 1755	04/06/2001	501019

PAY EXACTLY ****$1,276.00

PAY One Thousand Two Hundred Seventy Six & 00/100 Dollars- Void if not processed in 90 days -

TO THE ORDER OF COMMISSIONER OF PATENTS
AND TRADEMARKS

⑈501019⑈ ⑆122100024⑆ ⑈0591⑈

Please type a plus sign (+) inside this box → [+]

PTO/SB/05 (11-00)
Approved for use through 10/31/2002. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	29288.0300
First Inventor	Osamu SHIBATA, et al.
Title	COPYRIGHT PROTECTION SYSTEM, ENCRYPTION...
Express Mail Label No.	EM339435647US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, D.C. 20231

1. ☑ Fee Transmittal Form (e.g., PTO/SB/17) *(Submit an original, and a duplicate for fee processing)*
2. □ Applicant claims small entity status. See 37 CFR 1.27.
3. ☑ Specification *[Total Pages* 54 *]* *(preferred arrangement set forth below)*
   - Descriptive title of the invention
   - Cross Reference to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to sequence listing, a table, or a computer program listing appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
4. ☑ Drawing(s) *(35 U.S.C. 113)* *[Total Sheets* 9 *]*
5. Oath or Declaration *[Total Pages* ___ *]*
   a. □ Newly executed (original or copy)
   b. □ Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional with Box 18 completed)*
      i. □ DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. ☑ Application Data Sheet. See 37 CFR 1.76
7. □ CD-ROM or CD-R in duplicate, large table or Computer Program *(Appendix)*
8. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. □ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. □ CD-ROM or CD-R (2 copies); or
      ii. □ paper
   c. □ Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. □ Assignment Papers (cover sheet & document(s))
10. □ 37 CFR 3.73(b) Statement *(when there is an assignee)* □ Power of Attorney
11. □ English Translation Document *(if applicable)*
12. ☑ Information Disclosure Statement (IDS)/PTO-1449 ☑ Copies of IDS Citations
13. □ Preliminary Amendment
14. ☑ Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
15. ☑ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. □ Request and Certification under 35 U.S.C. 122 (b)(2)(B)(i). Applicant must attach form PTO/SB/35 or its equivalent.
17. □ Other:

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in a preliminary amendment, or in an Application Data Sheet under 37 CFR 1.76:*

□ Continuation □ Divisional □ Continuation-in-part (CIP) of prior application No.: ______/__________

Prior application information: Examiner __________ *Group / Art Unit* __________

For CONTINUATION OR DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

19. CORRESPONDENCE ADDRESS

☒ *Customer Number or Bar Code Label* 20322 *(Insert Customer No. or Attach bar code label here)* or □ *Correspondence address below*

Name	Michael K. Kelly SNELL & WILMER, LLP				
Address	One Arizona Center 400 E. Van Buren Street				
City	Phoenix	*State*	AZ	*Zip Code*	85004-2202
Country	USA	*Telephone*	602-382-6291	*Fax*	602-382-6070

Name (Print/Type)	Michael K. Kelly	*Registration No. (Attorney/Agent)*	32,848
Signature	Michael K. Kelly	*Date*	4/6/01

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

PTO/SB/17 (11-00)
Approved for use through 10/31/2002. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL for FY 2001

Patent fees are subject to annual revision.

TOTAL AMOUNT OF PAYMENT	$1,276.00

C mplete if Known

Application Number	To be assigned
Filing Date	April 6, 2001
First Named Inventor	Osamu SHIBATA, et al.
Examiner Name	To be assigned
Group Art Unit	To be assigned
Attorney Docket No.	29288.0300

METHOD OF PAYMENT

1. ☒ The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:

Deposit Account Number	19-2814
Deposit Account Name	Snell and Wilmer, LLP

☒ Charge Any Additional Fee Required Under 37 CFR §§ 1.16 and 1.17

☐ Applicant claims small entity status. See 37 CFR § 1.27

2. ☒ Payment Enclosed:

☒ Check ☐ Credit card ☐ Money Order ☐ Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	710	201	355	Utility filing fee	710.00
106	320	206	160	Design filing fee	
107	490	207	245	Plant filing fee	
108	710	208	355	Reissue filing fee	
114	150	214	75	Provisional filing fee	
				SUBTOTAL (1)	$710.00

2. EXTRA CLAIM FEES

			Extra Claims		Fee from below		Fee Paid
Total Claims	47	-20** =	27	X	18.00	=	486.00
Independent Claims	4	- 3** =	1	X	80.00	=	80.00
Multiple Dependent						=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
103	18	203	9	Claims in excess of 20
102	80	202	40	Independent claims in excess of 3
104	270	204	135	Multiple dependent claim, if not paid
109	80	209	40	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) $566.00

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet	
139	130	139	130	Non - English specification	
147	2,520	147	2,520	For filing a request for *ex parte* reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for reply within first month	
116	390	216	195	Extension for reply within second month	
117	890	217	445	Extension for reply within third month	
118	1,390	218	695	Extension for reply within fourth month	
128	1,890	228	945	Extension for reply within fifth month	
119	310	219	155	Notice of Appeal	
120	310	220	155	Filing a brief in support of an appeal	
121	270	221	135	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive - unavoidable	
141	1,240	241	620	Petition to revive - unintentional	
142	1,240	242	620	Utility issue fee (or reissue)	
143	440	243	220	Design issue fee	
144	600	244	300	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Processing fee under 37 CFR § 1.17(q)	
126	180	126	180	Submission of Information Disclosure Statement	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	710	246	355	Filing a submission after final rejection (37 CFR § 1.129(a))	
149	710	249	355	For each additional invention to be examined (37 CFR § 1.129(b))	
179	710	279	355	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application	

Other fee (specify) ______________________

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3)

SUBMITTED BY

Complete *(if applicable)*

Name (Print/Type)	Michael K. Kelly	*Registration No. (Attorney/Agent)*	32,848	*Telephone*	602-382-6291
Signature				*Date*	4/6/01

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Snell & Wilmer
L.L.P.
LAW OFFICES

One Arizona Center
Phoenix, Arizona 85004-2202
(602) 382-6000
Fax: (602) 382-6070
www.swlaw.com

PHOENIX, ARIZONA
TUCSON, ARIZONA
IRVINE, CALIFORNIA
SALT LAKE CITY, UTAH
DENVER, COLORADO
LAS VEGAS, NEVADA

FACSIMILE TRANSMISSION

TIME IN: 1 35 AP
TIME OUT:

DATE: November 17, 2003

TO:

Name	Fax Number	Phone Number
Cliff Congo Office of Petitions - USPTO	**703-308-6916**	703-305-0272

FROM: Julie Eslick PHONE: 602-382-6854

RE: U.S. Serial No. 09/828,559 - Petition Under CFR 1.181

MESSAGE:

Cliff:

Per our conversation, attached is a copy of our petition which was filed on August 12, 2003. If you need anything further, please do not hesitate to contact me. Please confirm receipt of this transmission by return facsimile. Thanks.

Julie A. Eslick
Patent & Trademark Assistant

ORIGINAL DOCUMENT:	Will not be sent	NUMBER OF PAGES (Including Cover):	77
CONFIRMATION NO.:		CLIENT MATTER NO.:	29288.0300
PLEASE RETURN TO:	Julie Eslick at 16107	PERSONAL FAX:	No
REQUESTOR:	Julie Eslick	DIRECT LINE:	602-382-6854

**IF YOU HAVE NOT PROPERLY RECEIVED THIS TELECOPY, PLEASE CALL US AT (602) 382-6075.
OUR FACSIMILE NUMBER IS (602) 382-6070.**

Part II
of 77

THE INFORMATION CONTAINED
THE USE OF THE INDIVIDUAL
EMPLOYEE OR AGENT RESPO
DISTRIBUTION OR COPYING O
PLEASE IMMEDIATELY NOTIFY
SERVICE. THANK YOU.

CONFIDENTIAL INFORMATION INTENDED ONLY FOR
SAGE IS NOT THE INTENDED RECIPIENT, OR THE
RE HEREBY NOTIFIED THAT ANY DISSEMINATION,
IAVE RECEIVED THIS COMMUNICATION IN ERROR,
US AT THE ABOVE ADDRESS VIA THE U.S. POSTAL

#4

INVENTOR INFORMATION

Inventor One Given Name:: Osamu
Family Name:: SHIBATA
Postal Address Line One:: 211, Shonanryo, 1-6-22, Kikusuidori,
Postal Address Line Two:: Moriguchi-shi
City:: Osaka
Country:: Japan
Postal or Zip Code:: 570-0032
City of Residence:: Osaka
Country of Residence:: Japan
Citizenship Country:: Japan
Inventor Two Given Name:: Tsutomu
Family Name:: SEKIBE
Postal Address Line One:: 5-49-34, Yamanoue, Hirakata-shi,
City:: Osaka
Country:: Japan
Postal or Zip Code:: 573-0047
City of Residence:: Osaka
Country of Residence:: Japan
Citizenship Country:: Japan

CORRESPONDENCE INFORMATION

Correspondence Customer Number:: 20322
Fax One:: 602-382-6070
Electronic Mail One:: mkelly@swlaw.com

APPLICATION INFORMATION

Title Line One:: COPYRIGHT PROTECTION SYSTEM, ENCRYPTION
Title Line Two:: DEVICE, DECRYPTION DEVICE AND RECORDING
Title Line Three:: MEDIUM
Total Drawing Sheets:: 9
Formal Drawings?:: Yes
Application Type:: Utility
Docket Number:: 29288.0300
Secrecy Order in Parent Appl.?:: No

REPRESENTATIVE INFORMATION

Representative Customer Number:: 20322

PRIOR FOREIGN APPLICATIONS

Foreign Application One:: 2000-105525
Filing Date:: 04-06-2000
Country:: Japan
Priority Claimed:: Yes

#4

P24493

COPYRIGHT PROTECTION SYSTEM, ENCRYPTION DEVICE, DECRYPTION DEVICE, AND RECORDING MEDIUM

BACKGROUND OF THE INVENTION

1. FIELD OF THE INVENTION:

The present invention relates to a communication system performing cryptographic communication in which digital contents, such as music, images, videos, and games, having a decryption limitation are transferred using a common key which is shared by devices so that the decryption of the digital contents is forbidden when the updating of the decryption limitation is unauthorized. More particularly, the present invention relates to a copyright protection system, an encryption device, a decryption device, and a recording medium for protecting copyrights by associating update information on the decryption limitation with the common key.

2. DESCRIPTION OF THE RELATED ART:

Recently, the development of digital information compression technologies and the explosive pervasion of communication infrastructures have realized that contents, such as music, images, videos, and games, are distributed in the form of digital information via communication lines to homes.

The digital information distributed via communication lines is in the form of data which is not stored in any medium. Therefore, the flexibility of distribution service forms is dramatically increased. Distribution services can not only provide digital contents but also limit the use of the contents (e.g., the limited number of uses and the limited period of use). A wide variety of distribution service forms are contemplated.

The establishment of distribution systems, in which the copyrights of digital contents and the profits of distributors are protected, requires solving how to prevent unauthorized actions, such as fraud possession by communication intercept, eavesdropping, pretending, or the like, and illegal duplications and falsifications of received data stored in a recording medium. Such a solution would be provided by copyright protection technologies, such as an encryption/authentication technique performing the identification of authentic systems, data scramble, and the like.

There are a variety of conventional copyright protection technologies. A typical technology is a challenge-response type mutual authentication system in which random numbers and response values are exchanged between a data encryption device and a data decryption device so that both devices are mutually authenticated, and data is transferred when the authentication is established.

The term "decryption limitation" as used herein refers to information on whether contents transferred from an encryption device to a decryption device are allowed to be used (e.g., reproduce to make a sound). For example, when contents are associated with the number of times the contents can be reproduced, such a number of times is a decryption limitation.

The term "updating of a decryption limitation" as used herein refers to a rule which is used in updating a decryption limitation. For example, for contents associated with the number of times the contents can be reproduced (e.g., N times), such a number of times is a decryption limitation transferred from an encryption device to a decryption device, and the updating of the decryption limitation means that the number of times is reduced by one.

The term "update information on a decryption limitation" as used herein refers to a decryption limitation which is updated. For example, for contents associated with the number of times the contents can be reproduced (e.g., N times), the number of times which is a decryption limitation transferred from an encryption device to a decryption device, is updated so that the update information on the decryption limitation is rewritten to "N-1 times".

A typical cryptographic communication system in which digital contents having a decryption limitation are transferred using the above-described mutual authentication technique, will be described. An encryption device and a decryption device are mutually authenticated. Only when the authentication is established, the decryption limitation is encrypted and then transferred from the encryption device to the decryption device. The decryption device interprets the decryption limitation to determine whether the digital contents can be decrypted, and updates the decryption limitation. The update information on the updated decryption limitation is encrypted and transferred to the encryption device. Thereafter, the contents are encrypted and loaded into the decryption device which in turn decrypts the loaded contents.

A decryption limitation should be correctly updated. In other words, update information on a decryption limitation decrypted by a decryption device should be received by an authenticated encryption device. If a decryption limitation is not correctly updated, i.e., update information on a decryption limitation decrypted by a decryption device is received by a false encryption device pretending to be an authenticated encryption device, the decryption limitation is not updated by the authenticated encryption device and contents loaded from the authenticated encryption device are decrypted by the decryption device in an unauthorized manner. Therefore, a system is required in which, when update information on a decryption limitation decrypted by a decryption device is received by a false encryption device pretending to be an authenticated encryption device, the decryption device is forbidden to decrypt contents loaded from the authenticated encryption device.

In the above-described mutual authentication technique, a determination is made only as to whether communicating devices are authenticated. Whether a decryption limitation is currently updated is not determined. Therefore, an unauthorized action cannot be prevented. If update information on a decryption limitation decrypted by a decryption device is received by a false encryption device pretending to be an authenticated encryption device, the decryption limitation is not updated by the authenticated encryption device, and nevertheless contents loaded from the authenticated encryption device cannot be decrypted by the decryption device in an unauthorized manner.

SUMMARY OF THE INVENTION

According to one aspect of the present invention, a copyright protection system comprises an encryption device and a decryption device, wherein cryptographic communication is performed between the encryption device and the decryption device using a contents key. The encryption device includes a contents storage section for storing contents, a first contents key generation section for generating the contents key based on a second decryption limitation obtained by updating a first decryption limitation, and a first encryption section for encrypting the contents using the contents key and outputting the encrypted contents. The decryption device includes a second contents key generation section for generating the contents key from the second decryption limitation, and a first decryption section for decrypting the encrypted contents using the contents key generated by the second contents key generation section.

In one aspect of this invention, the decryption device further includes a decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and a second encryption section for encrypting the second decryption limitation using a time-varying key, and outputting the first encrypted decryption limitation. The encryption device further includes a second decryption section for decrypting the first encrypted decryption limitation transferred from the second encryption section using the time-varying key to generate the second decryption limitation. The first contents key generation section generates the contents key based on the second decryption limitation generated by the second decryption section.

In one aspect of this invention, the encryption device further includes a first common key storage section for storing a common key, a decryption limitation storage section for storing the first decryption limitation, a first random number generation section for generating a first random number, a first mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device, a first time-varying key generation section for generating the time-varying key using the first random number and the second random number in response to the authentication by the first mutual authentication section, and a third encryption section for encrypting the first decryption limitation using the time-varying key and outputting the second encrypted decryption limitation. The decryption device further includes a second common key storage section for storing the common key, a second random number generation section for generating the second random number, a second mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and the first random number, a second time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the second mutual authentication section, and a third decryption section for decrypting the second encrypted decryption limitation using the time-varying key.

In one aspect of this invention, the decryption device further includes a first decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and a second contents key generation section for generating the contents key based on the second decryption limitation updated by the first decryption limitation updating section. The encryption device further includes a second decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with the decryption limitation updating rule in response to the updating of the first decryption limitation by the first decryption limitation updating section. The first contents key generation section generates the contents key based on the second decryption limitation updated by the first decryption limitation updating section.

In one aspect of this invention, the encryption device further includes a first common key storage section for storing a common key, a decryption limitation storage section for storing the first decryption limitation, a first random number generation section for generating a first random number, a first mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device, a first time-varying key generation section for generating a time-varying key using the first random number and the second random number in response to the authentication by the first mutual authentication section, and a second encryption section for encrypting the first decryption limitation using the time-varying key and outputting an encrypted decryption limitation. The decryption device further includes a second common key storage section for storing the common key, a second random number generation section for generating the second random number, a second mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and the first random number, a second time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the second mutual authentication section, and a second decryption section for decrypting the encrypted decryption limitation using the time-varying key.

In one aspect of this invention, the second decryption limitation updating section updates the first decryption limitation to the second decryption limitation in advance. The first contents key generation section generates the contents key from the second decryption limitation. The second decryption limitation updating section stores the second decryption limitation in the decryption limitation storage section in response to the start of processing by the first encryption section.

In one aspect of this invention, the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers and the common key.

In one aspect of this invention, the first and second contents key generation sections generate the contents key based on the second decryption limitation and the time-varying key.

In one aspect of this invention, the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device. The first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers and the respective data sequence key.

In one aspect of this invention, the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device. The first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers, the common key, and the respective data sequence key.

In one aspect of this invention, the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device. The first and second contents key generation sections generate the contents key based on the second decryption limitation and the respective data sequence key.

In one aspect of this invention, the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device. The first and second contents key generation section generate the contents key based on the second decryption limitation, the time-varying key, and the respective data sequence key.

In one aspect of this invention, the first and second mutual authentication sections mutually authenticate the decryption device and the encryption device, respectively, by communication in accordance with a challenge-response type authentication protocol.

According to another aspect of the present invention, an encryption device for performing cryptographic communication in association with a decryption device using a contents key, comprises a contents storage section for storing contents, a contents key generation section for generating the contents key based on a second decryption limitation obtained by updating a first decryption limitation, and a first encryption section for encrypting the contents using the contents key and outputting the encrypted contents.

In one aspect of this invention, the encryption device further includes a decryption section for decrypting the first encrypted decryption limitation transferred from the decryption device using the time-varying key to generate the second decryption limitation, and the contents key generation section generates the contents key based on the second decryption limitation generated by the decryption device.

In one aspect of this invention, the encryption device further includes a common key storage section for storing a common key, a decryption limitation storage section for storing the first decryption limitation, a first random number generation section for generating a first random number, a mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device, a time-varying key generation section for generating the time-varying key using the first random number and the second random number in response to the authentication by the mutual authentication section, and a second encryption section for encrypting the first decryption limitation using the time-varying key and outputting the second encrypted decryption limitation.

In one aspect of this invention, the encryption device further includes a decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule in response to the updating of a decryption limitation by the decryption device. The contents key generation section generates the contents key based on the second decryption limitation obtained by the decryption limitation updating section.

In one aspect of this invention, the encryption device further includes a common key storage section for storing a common key, a decryption limitation storage section for storing the first decryption limitation, a first random number generation section for generating a first random number, a mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device, a time-varying key generation section for generating a time-varying key using the first random number and the second random number in response to the authentication by the mutual authentication section, and a second encryption section for encrypting the first decryption limitation using the time-varying key and outputting an encrypted decryption limitation.

In one aspect of this invention, the decryption limitation updating section updates the first decryption limitation to the second decryption limitation in advance. The decryption limitation updating section outputs the second decryption limitation to the contents key generation section. The contents key generation section generates the contents key from the second decryption limitation. The decryption limitation updating section stores the second decryption limitation in the decryption limitation storage section in response to the start of processing by the first encryption section.

In one aspect of this invention, the time-varying key generation section generates the time-varying key based on the first and second random numbers and the common key.

In one aspect of this invention, the contents key generation section generates the contents key based on the second decryption limitation and the time-varying key.

In one aspect of this invention, the encryption device further includes a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device, the time-varying key generation section generates the time-varying key based on the first and second random numbers and the data sequence key.

In one aspect of this invention, the encryption device further includes a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device. The time-varying key generation section generates the time-varying key based on the first and second random numbers, the common key, and the data sequence key.

In one aspect of this invention, the encryption device further includes a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device. The contents key generation section generates the contents key based on the second decryption limitation and the data sequence key.

In one aspect of this invention, the encryption device further includes a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device. The contents key generation section generates the contents key based on the second decryption limitation, the time-varying key, and the data sequence key.

According to another aspect of the present invention, a decryption device for performing cryptographic communication in association with an encryption device using a contents key, comprises a contents key generation section for generating the contents key from a second decryption limitation, and a first decryption section for decrypting encrypted contents using the contents key generated by the contents key generation section.

In one aspect of this invention, the decryption device further includes a decryption limitation updating section for updating a first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and an encryption section for encrypting the second decryption limitation using a time-varying key, and outputting the first encrypted decryption limitation.

In one aspect of this invention, the decryption device further includes a common key storage section for storing the common key, a random number generation section for generating the second random number, a mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and a first random number, a time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section, and a second decryption section for decrypting a first encrypted decryption limitation using the time-varying key.

In one aspect of this invention, the decryption device further includes a decryption limitation updating section for updating the first decryption limitation to a second decryption limitation in accordance with a decryption limitation updating rule. A contents key generation section for generating the contents key based on the second decryption limitation updated by the decryption limitation updating section.

In one aspect of this invention, the decryption device further includes a second common key storage section for storing the common key, a second random number generation section for generating the second random number, a mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and a first random number, a time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section, and a second decryption section for decrypting encrypted decryption limitation using the time-varying key.

In one aspect of this invention, the time-varying key generation section generates the time-varying key based on the first and second random numbers and the common key.

In one aspect of this invention, the contents key generation section generates the contents key based on the second decryption limitation and the time-varying key.

In one aspect of this invention, the decryption device further includes a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the decryption device. The time-varying key generation section generates the time-varying key based on the first and second random numbers and the data sequence key.

In one aspect of this invention, the decryption device further includes a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the decryption device. The time-varying key generation section generates the time-varying key based on the first and second random numbers, the common key, and the data sequence key.

In one aspect of this invention, the decryption device further includes a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the decryption device. The contents key generation section generates the contents key based on the second decryption limitation and the data sequence key.

In one aspect of this invention, the decryption device further includes a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the decryption device. The contents key generation section generates the contents key based on the second decryption limitation, the time-varying key, and the data sequence key.

According to another aspect of the present invention, there is provided a recording medium storing a program for use in causing a computer to perform cryptographic communication with an encryption device using a contents key. The program causes the computer to function as a contents key generation section for generating the contents key from a second decryption limitation, and a first decryption section for decrypting encrypted contents using the contents key generated by the contents key generation section.

In one aspect of this invention, the program causes the computer to further function as a decryption limitation updating section for updating a first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and an encryption section for encrypting the second decryption limitation using a time-varying key, and outputting a first encrypted decryption limitation.

In one aspect of this invention, the program causes the computer to further function as a common key storage section for storing the common key, a random number generation section for generating a second random number, a mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and a first random number, a time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section, and a second decryption section for decrypting a first encrypted decryption limitation using the time-varying key.

In one aspect of this invention, the program causes the computer to further function as a decryption limitation updating section for updating a first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and a contents key generation section for generating the contents key based on the second decryption limitation obtained by the decryption limitation updating section.

In one aspect of this invention, the program causes the computer to further function as a second common key storage section for storing the common key, a second random number generation section for generating the second random number, a mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and a first random number, a time-varying key generation section for generating a time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section, and a second decryption section for decrypting encrypted decryption limitation using the time-varying key.

In one aspect of this invention, the time-varying key generation section generates the time-varying key based on the first and second random numbers and the common key.

In one aspect of this invention, the contents key generation section generates the contents key based on the second decryption limitation and the time-varying key.

In one aspect of this invention, the program causes the computer to further function as a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device. The time-varying key generation section generates the time-varying key based on the first and second random numbers and the data sequence key.

In one aspect of this invention, the program causes the computer to further function as a sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device. The time-varying key generation section generates the time-varying key based on the first and second random numbers, the common key, and the data sequence key.

In one aspect of this invention, the program causes the computer to further function as a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device. The contents key generation section generates the contents key based on the second decryption limitation and the data sequence key.

In one aspect of this invention, the program causes the computer to further function as a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device. The contents key generation section generates the contents key based on the second decryption limitation, the time-varying key, and the data sequence key.

Thus, the invention described herein makes possible the advantages of (1) providing a copyright protection system, an encryption device, a decryption device, and a recording medium, in which a decryption limitation is reliably updated and unauthorized decryption of digital contents is prevented, and (2) providing a copyright protection system, an encryption device, a decryption device, and a recording medium, in which, when update information on a decryption limitation updated by a decryption device is received by a false encryption device pretending to be an authenticated encryption device (instead of the authenticated encryption device), contents loaded from the authenticated encryption device cannot be decrypted by the decryption device.

These and other advantages of the present invention will become apparent to those skilled in the art upon reading and understanding the following detailed description with reference to the accompanying figures.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a diagram showing a configuration of a system according to Example 1 of the present invention.

Figure 2 is a flowchart showing processing steps of the system of Example 1.

Figure 3 is a diagram showing a configuration of a system according to Example 2 of the present invention.

Figure 4 is a diagram showing a configuration of a system according to Example 3 of the present invention.

Figure 5 is a diagram showing a configuration of a system according to Example 4 of the present invention.

Figure 6 is a diagram showing a configuration of a system according to Example 5 of the present invention.

Figure 7 is a diagram showing a configuration of a system according to Example 6 of the present invention.

Figure 8 is a diagram showing a configuration of a system according to Example 7 of the present invention.

Figure 9 is a diagram showing another configuration of the system of Example 7.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Hereinafter, the present invention will be described by way of illustrative examples with reference to the accompanying drawings. In the present invention, a decryption limitation is used to generate a common key which is used to encrypt digital contents.

(Example 1)

Figure 1 is a diagram showing a configuration of a system according to Example 1 of the present invention, in which cryptographic communication is performed between an encryption device 101 and a decryption device 102.

The encryption device 101 includes: a common key storage section 103 for storing a common key UK; a decryption limitation storage section 111 for storing a decryption limitation; a contents storage section 121 for storing contents CT; a random number generation section 105 for generating a random number R1; a mutual authentication section 107 for performing mutual authentication with the decryption device 102 using the random number R1, a random number R2 transferred from the decryption device 102, and the common key UK; a time-varying key generation section 109 for generating a time-varying key VK every time the mutual authentication using the random numbers R1 and

R2 is performed in the mutual authentication section 107; an encryption section 113 for encrypting the decryption limitation S1 using the time-varying key VK, and outputting an encrypted decryption limitation S2; a decryption section 115 for decrypting an encrypted decryption limitation S3 transferred from an encryption section 116 of the decryption device 102, using the time-varying key VK, to a decryption limitation S4, and writing the decryption limitation S4 to the decryption limitation storage section 111; a contents key generation section 117 for generating a contents key CK from the decryption limitation S4; and an encryption section 119 for encrypting the contents CT using the contents key CK, and outputting encrypted contents S5.

The decryption device 102 includes: a common key storage section 104 for storing the common key UK; a random number generation section 106 for generating the random number R2; a mutual authentication section 108 for performing mutual authentication with the encryption device 101 using the random numbers R1 and R2 and the common key UK; a time-varying key generation section 110 for generating the time-varying key VK in response to the mutual authentication in the mutual authentication section 108; a decryption section 114 for decrypting the encrypted decryption limitation S2 using the time-varying key VK; a decryption limitation updating section 112 for updating the decryption limitation S4 based on a decryption limitation updating rule using the decryption limitation S1 decrypted in the decryption section 114; an encryption section 116 for encrypting the decryption limitation S4 using the time-varying key VK, and outputting the encrypted decryption limitation S3; a contents key generation section 118 for generating the contents key CK from the decryption limitation S4; and a decryption section 120 for decrypting the encrypted contents S5 using the contents key CK, and outputting the contents CT.

The encryption device 101 and the decryption device 102 include the respective common key storage sections 103 and 104 to hold the same common key UK. The same common key UK is stored in the common key storage sections 103 and 104 in advance, or produced in a production process.

The encryption device 101 includes the decryption limitation storage section 111 for storing the decryption limitation S1 and the contents storage section 121 for storing the contents CT. The common key storage section 103, the decryption limitation storage section 111, and the contents storage section 121 are provided in a protect region which is not accessed directly from the outside of the encryption device 101.

Figure 2 is a flowchart showing processing steps of the system 100 of Example 1. The processing steps of the system 100 including the encryption device 101 and the decryption device 102 are hereinafter described with reference to Figures 1 and 2.

The encryption device 101 and the decryption device 102 include the respective random number generation section 105 and 106 which generate the random numbers R1 and R2 which are independent of each other. The random numbers R1 and R2 are exchanged between the encryption device 101 and the decryption device 102. The decryption device 102 generates a response value V1 using the random number R1 and the common key UK. The encryption device 101 generates a response value V2 using the random number R2 and the common key UK. The response values V1 and V2 are exchanged between the encryption device 101 and the decryption device 102. The mutual authentication sections 107 and 108 compares the response value V1 with the response value V2 to determine whether the other device is authentic. In this manner, a challenge-response type mutual authentication is performed (S201).

A determination is made whether the authentication is established in the encryption device 101 and the decryption device 102 (S202). If it is determined that the authentication is not established (NO in S202), the process is ended. If it is determined that the authentication is established (YES in S202), the time-varying key generation sections 109 and 110 generate the same time-varying key VK, which is changed at every mutual authentication, from the respective random numbers R1 and R2 (S203). Thereafter, the decryption limitation S1 stored in the decryption limitation storage section 111 of the encryption device 101 is encrypted in the encryption section 113 using the time-varying key VK, and the encrypted decryption limitation S2 is transferred to the decryption device 102 (S204).

The decryption section 114 decrypts the received decryption limitation S2 using the time-varying key VK (S205). The decryption limitation updating section 112 updates the decryption limitation S1 decrypted in the decryption section 114, in accordance with the decryption limitation updating rule (S206). The encryption section 116 encrypts the updated decryption limitation S4 using the time-varying key VK (S207), and outputs the encrypted decryption limitation S3 to the encryption device 101. The decryption section 115 decrypts the transferred encrypted decryption limitation S3 using the time-varying key VK, and stores the updated decryption limitation S4 in the decryption limitation storage section 111 (S208).

The contents key generation section 117 generates the contents key CK from the decryption limitation S4 (S209). When the contents CT stored in the contents storage section 121 are transferred from the encryption device 101 to the decryption device 102, the encryption section 119 encrypts the contents CT using the contents key CK (S210). The contents key generation section 118 generates the contents key CK from the decryption limitation S4 (S211). The encryption section 120 in the decryption device 102 decrypts the encrypted contents S5 using the contents key CK (S212).

In Example 1, contents are transferred from an encryption device to a decryption device after authentication is established at a single time. Alternatively, mutual authentication may be performed every time the transfer of contents between encryption and decryption devices occurs. In Example 1, the time-varying key VK is generated using the random numbers R1 and R2 which are used in mutual authentication. Alternatively, the time-varying key VK may be generated using the response values V1 and V2.

Different algorithms or the same algorithm may be used to encrypt and decrypt a decryption limitation and contents. An example of an algorithm is DES (Data Encryption Standard).

Different algorithms or the same algorithm may be used to generate a time-varying key and a contents key. An example of an algorithm is a one-way function, such as SHA (Secure Hash Algorithm).

In Example 1, for the sake of simplicity, transmission and reception are performed by the mutual authentication sections 107 and 108, the encryption section 113, the decryption section 114, the decryption section 115, the encryption section 116, the encryption section 119, and the decryption section 120. The transmission and reception are typically managed by control sections 122 and 123. The same applies to examples described later.

As described above, the copyright protection system of Example 1 performs cryptographic communication by associating the copyrighted contents CT with update information on a decryption limitation (the decryption limitation S4). Therefore, the contents CT cannot be decrypted unless the decryption limitation S1 is updated in an authorized manner.

(Example 2)

Figure 3 is a diagram showing a copyright protection system 200 according to Example 2 of the present invention. In Figure 2, the same components as those in Figure 1 are indicated by the same reference numerals. The description thereof is thus omitted.

In the copyright protection system 100, a decryption limitation S4 updated in a decryption limitation updating section 112 is encrypted/decrypted and then transferred as is in the copyright protection system 100. In the copyright protection system 200, the decryption limitation S4 is not stored in a decryption limitation storage section 111, but a decryption limitation updating section 223 is provided in an encryption device 201.

A decryption limitation updating section 212 in a decryption device 202 transfers only a decryption limitation updating instruction CC to update a decryption limitation S1 to the decryption limitation updating section 223. The decryption limitation updating section 223 receives the transferred decryption limitation updating instruction CC, updates the decryption limitation S1, and stores the updated decryption limitation S4 in a decryption limitation storage section 211.

As described above, the copyright protection system 200 does not need to transfer the updated decryption limitation S4 associated with generation of the contents key CK from the decryption device 202 to the encryption device 201. Therefore, the secrecy of the decryption limitation S4 is increased. Further, an encryption section and a decryption section (e.g., 116 and 115, respectively, in Figure 1) which involve transfer of the updated decryption limitation S4 can be deleted, thereby making it possible to reduce the size of the system.

(Example 3)

Figure 4 is a diagram showing a copyright protection system 300 according to Example 3 of the present invention. In Figure 4, the same components as those in Figure 1 are indicated by the same reference numerals. The description thereof is thus omitted.

In the copyright protection system 200 of Figure 2, the decryption limitation updating section 223 in the encryption device 201 updates the decryption limitation S1 according to the updating instruction CC from the decryption limitation updating section 212. Unlike the copyright protection system 200, in the copyright protection system 300, the decryption limitation updating section 323 updates a decryption limitation S1 previously stored in a decryption limitation storage section 311 in an encryption device 301. A contents key generation section 117 generates a contents key CK using an updated decryption limitation S4. The decryption limitation updating section 323 stores the updated decryption limitation S4 in a decryption limitation storage section 311 in response to an encryption section 319 starting encryption of contents CT.

As described above, in the copyright protection system 300 of Example 3, the decryption limitation S1 is not updated according to the instruction from a decryption device 302, but the decryption limitation updating section 323 previously updates the decryption limitation S1 and the contents key generation section 117 generates the contents key CK. Therefore, the processing steps can be reduced.

(Example 4)

Figure 5 is a diagram showing a copyright protection system 400 according to Example 4 of the present invention. In Figure 5, the same components as those in Figure 1 are indicated by the same reference numerals. The description thereof is thus omitted.

In the copyright protection system 400, time-varying key generation sections 409 and 410 generate a time-varying key VK using a common key UK in addition to random numbers R1 and R2. For example, the time-varying key VK is generated by an exclusive OR of the random numbers R1 and R2 and the common key UK, and converting the result using a one-way function.

As described above, according to the copyright protection system 400, the time-varying key VK is generated not only by the random numbers R1 and R2 which can be externally monitored, but in association with the secret common key UK. Therefore, the time-varying key VK is difficult to infer, thereby making it possible to improve the secrecy of the time-varying key VK.

(Example 5)

Figure 6 is a diagram showing a copyright protection system 500 according to Example 5 of the present invention. In Figure 6, the same components as those in Figure 1 are indicated by the same reference numerals. The description thereof is thus omitted.

In the copyright protection system 500, contents key generation sections 517 and 518 generate a contents key CK using a time-varying key VK in addition to an updated decryption limitation S4. For example, the contents key CK is generated by an exclusive OR of the decryption limitation S4 and the time-varying key VK, and converting the result using a one-way function.

As described above, according to the copyright protection system 500 of Example 5, the contents key CK is generated not only by the updated decryption limitation S4, but in association with the time-varying key VK which time-sequencially varies in each mutual authentication. Therefore, the cryptographic security of contents can be improved.

(Example 6)

Figure 7 is a diagram showing a copyright protection system 600 according to Example 6 of the present invention. In Figure 7, the same components as those in Figure 1 are indicated by the same reference numerals. The description thereof is thus omitted.

In the copyright protection system 600, an encryption device 601 and a decryption device 602 include data sequence key generation sections 625 and 626, respectively, which generate a data sequence key TK1 from all or part of data input to or output from the encryption device 601 and the decryption device 602. In this case, such input or output data include random numbers R1 and R2, response values V1 and V2, encrypted decryption limitations S2 and S3, and encrypted contents S5. The data sequence key TK1 is additionally used to generate a contents key CK in contents key generation sections 617 and 618.

The data sequence key TK1 may be generated by counting a High or Low level of each input/output data, for example. The time-varying key VK may be generated by an exclusive OR of the random numbers R1 and R2 and the data sequence key TK1, and converting the result using a one-way function. All input/output data are not necessarily used to generate the data sequence key TK1. A part of the input/output data may be used.

As described above, in the copyright protection system 600, data input to or output from the encryption device 601 and the decryption device 602 are monitored, and the data sequence key TK1 common to both devices is generated from the input/output data so that the generated data sequence key TK1 is associated with generation of the contents key CK. Therefore, since the same data is input to and output from an encryption device and a decryption device in a cryptographic system, pretending can be prevented.

(Example 7)

Figure 8 is a diagram showing a configuration of a system 800 in which cryptographic communication is performed between an encryption device 101 and a decryption device 102. Referring to Figure 8, the encryption device 101 and the decryption device 102 are directly connected to each other. In Figure 8, the same components as those in Figure 1 are indicated by the same reference numerals. The description thereof is thus omitted.

The system 800 includes a contents reproduction device 801 for reproducing contents. The the encryption device 101 is attached to the contents reproduction device 801. The contents reproduction device 801 further includes a decryption device 102 described in Example 1 and a reproduction section 802 for reproducing contents decrypted by the decryption device 102.

As described above, the decryption device 102 described in Example 1 may be included in the contents reproduction device 801. The encryption device 101 described in Example 1 is attached to the contents reproduction device 801. The encryption device 101 attached to the contents reproduction device 801 and the decryption device 102 included in the contents reproduction device 801 performs cryptographic communication as described in Example 1.

The contents reproduction device 801 may be a cellular telephone, an audio player, or a personal computer. The encryption device 101 may be a memory card. The encryption device 101 may be any of the encryption devices 201 through 601 described in Examples 2 through 6. The decryption device 102 may be any of the decryption devices 202 through 602 described in Examples 2 through 6.

The decryption device 102 may be operated in accordance with a program for operating the decryption device described in any of Examples 1 through 6, read from a recording medium 803 in which the program is recorded. The recording medium 803 may be a CD-ROM.

Figure 9 is a diagram showing another configuration of the system 800 in which cryptographic communication is performed between the encryption device 101 and the decryption device 102. Referring to Figure 9, the encryption device 101 and the decryption device 102 are directly connected to each other via an electric communication line. In Figure 9, the same components as those in Figures 1 and 8 are indicated by the same reference numerals. The description thereof is thus omitted.

Referring to Figure 9, the system 900 includes a contents reproduction device 801 for reproducing contents, and an electric communication line 903 connecting the contents reproduction device 801 and a server 901. The contents reproduction device 801 includes a decryption device 102 described in Example 1 and a reproduction section 802 for reproducing contents decrypted by the decryption device 102. An encryption device 101 described in Example 1 is attached to the server 901.

In this manner, the contents reproduction device 801 for reproducing contents and the server 901 are connected to each other via the electric communication line 903. The encryption device 101 is attached to the server 901. The encryption device 101 attached to the server 901 and the decryption device 102 included in the contents reproduction device 801 perform cryptographic communication via the electric communication line 903.

The electric communication line 903 may be the Internet or a local area network (LAN).

Similar to the example of Figure 8, the contents reproduction device 801 may be a cellular telephone, an audio player, or a personal computer. The encryption device 101 may be a memory card. The encryption device 101 may be any of the encryption devices 201 through 601 described in Examples 2 through 6. The decryption device 102 may be any of the decryption devices 202 through 602 described in Examples 2 through 6.

Similar to the example of Figure 8, the decryption device 102 may be operated in accordance with a program for operating the decryption device described in any of Examples 1 through 6, read from a recording medium 803 in which the program is recorded. The recording medium 803 may be a CD-ROM.

In Figure 9, the encryption device 101 and the decryption device 102 are connected to each other via the electric communication line 903. This invention is not limited to this. The encryption device 101 and the decryption device 102 may be connected to each other via a wireless communication line.

As described above, according to the present invention, a copyright protection system in which a decryption limitation is reliably updated and unauthorized decryption of digital contents is prevented, an encryption device, a decryption device, and a recording medium, can be provided.

Further, according to the present invention, a copyright protection system, an encryption device, a decryption device, and a recording medium can be provided, in which, when update information on a decryption limitation updated by a decryption device is received by a false encryption device pretending to be an authenticated encryption device (instead of the authenticated encryption device), advantageously contents loaded from the authenticated encryption device cannot be decrypted by the decryption device.

Further, according to the present invention, a copyright protection system, an encryption device, a decryption device, and a recording medium can be provided, in which cryptographic communication is performed by associating copyrighted contents with update information on a decryption limitation and, therefore, advantageously the contents cannot be decrypted unless the decryption limitation is updated in an authorized manner.

Further, according to the present invention, a copyright protection system, an encryption device, a decryption device, and a recording medium can be provided, in which updated decryption limitation associated with generation of a contents key does not need to be transferred from a decryption device to an encryption device and therefore, advantageously the secrecy of the decryption limitation is increased, and further, an encryption section and a decryption section which involve transfer of the updated decryption limitation can be deleted, thereby advantageously making it possible to reduce the size of the system.

Further, according to the present invention, a copyright protection system, an encryption device, a decryption device, and a recording medium can be provided, in which a decryption limitation is not updated according to an instruction from a decryption device, but rather a decryption limitation updating section previously updates the decryption limitation and a contents key generation section generates the contents key and, therefore, advantageously the processing steps can be reduced.

Further, according to the present invention, a copyright protection system, an encryption device, a decryption device, and a recording medium can be provided, in which a time-varying key is generated not only by random numbers which can be externally monitored, but also in association with a secret common key and, therefore, the time-varying key is difficult to infer, thereby advantageously making it possible to improve the secrecy of the time-varying key.

Further, according to the present invention, a copyright protection system, an encryption device, a decryption device, and a recording medium can be provided, in which data input to or output from an encryption device and a decryption device are monitored, and a data sequence key common to both devices is generated from the input/output data so that the generated data sequence key is associated with generation of a contents key and, therefore, pretending can be advantageously prevented.

Various other modifications will be apparent to and can be readily made by those skilled in the art without departing from the scope and spirit of this invention. Accordingly, it is not intended that the scope of the claims appended hereto be limited to the description as set forth herein, but rather that the claims be broadly construed.

WHAT IS CLAIMED IS:

1. A copyright protection system comprising:

an encryption device and a decryption device, wherein cryptographic communication is performed between the encryption device and the decryption device using a contents key,

wherein the encryption device includes

a contents storage section for storing contents,

a first contents key generation section for generating the contents key based on a second decryption limitation obtained by updating a first decryption limitation, and

a first encryption section for encrypting the contents using the contents key and outputting the encrypted contents, and

wherein the decryption device includes

a second contents key generation section for generating the contents key from the second decryption limitation, and

a first decryption section for decrypting the encrypted contents using the contents key generated by the second contents key generation section.

2. A copyright protection system according to claim 1,

wherein the decryption device further includes

a decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and

a second encryption section for encrypting the second decryption limitation using a time-varying key, and outputting the first encrypted decryption limitation,

wherein the encryption device further includes a second decryption section for decrypting the first encrypted decryption limitation transferred from the second encryption section using the time-varying key to generate the second decryption limitation,

wherein the first contents key generation section generates the contents key based on the second decryption limitation generated by the second decryption section.

3. A copyright protection system according to claim 2, wherein the encryption device further includes

a first common key storage section for storing a common key,

a decryption limitation storage section for storing the first decryption limitation,

a first random number generation section for generating a first random number,

a first mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device,

a first time-varying key generation section for generating the time-varying key using the first random number and the second random number in response to the authentication by the first mutual authentication section, and

a third encryption section for encrypting the first decryption limitation using the time-varying key and outputting the second encrypted decryption limitation, and

wherein the decryption device further includes

a second common key storage section for storing the common key, a second random number generation section for generating the second random number,

a second mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and the first random number,

a second time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the second mutual authentication section, and

a third decryption section for decrypting the second encrypted decryption limitation using the time-varying key.

4. A copyright protection system according to claim 1, wherein the decryption device further includes a first decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and

a second contents key generation section for generating the contents key based on the second decryption limitation updated by the first decryption limitation updating section,

wherein the encryption device further includes a second decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with the decryption limitation updating rule in response to the updating of the first decryption limitation by the first decryption limitation updating section,

the first contents key generation section generates the contents key based on the second decryption limitation updated by the first decryption limitation updating section.

5. A copyright protection system according to claim 4, wherein the encryption device further includes

a first common key storage section for storing a common key,

a decryption limitation storage section for storing the first decryption limitation,

a first random number generation section for generating a first random number,

a first mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device,

a first time-varying key generation section for generating a time-varying key using the first random number and the second random number in response to the authentication by the first mutual authentication section, and

a second encryption section for encrypting the first decryption limitation using the time-varying key and outputting an encrypted decryption limitation, and

wherein the decryption device further includes

a second common key storage section for storing the common key,

a second random number generation section for generating the second random number,

a second mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and the first random number, a second time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the second mutual authentication section, and

a second decryption section for decrypting the encrypted decryption limitation using the time-varying key.

6. A copyright protection system according to claim 5, wherein the second decryption limitation updating section updates the first decryption limitation to the second decryption limitation in advance,

the first contents key generation section generates the contents key from the second decryption limitation, and

the second decryption limitation updating section stores the second decryption limitation in the decryption limitation storage section in response to the start of processing by the first encryption section.

7. A copyright protection system according to claim 3, wherein the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers and the common key.

8. A copyright protection system according to claim 3, wherein the first and second contents key generation sections generate the contents key based on the second decryption limitation and the time-varying key.

9. A copyright protection system according to claim 3, wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key

based on a data sequence input to or output from the encryption device and the decryption device, and

wherein the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers and the respective data sequence key.

10. A copyright protection system according to claim 3, wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device, and

wherein the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers, the common key, and the respective data sequence key.

11. A copyright protection system according to claim 3, wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device, and

wherein the first and second contents key generation sections generate the contents key based on the second decryption limitation and the respective data sequence key.

12. A copyright protection system according to claim 3, wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the

encryption device and the decryption device, and

wherein the first and second contents key generation section generate the contents key based on the second decryption limitation, the time-varying key, and the respective data sequence key.

13. A copyright protection system according to claim 3, wherein the first and second mutual authentication sections mutually authenticate the decryption device and the encryption device, respectively, by communication in accordance with a challenge-response type authentication protocol.

14. An encryption device for performing cryptographic communication in association with a decryption device using a contents key, comprising:

a contents storage section for storing contents;

a contents key generation section for generating the contents key based on a second decryption limitation obtained by updating a first decryption limitation; and

a first encryption section for encrypting the contents using the contents key and outputting the encrypted contents.

15. An encryption device according to claim 14, further including a decryption section for decrypting the first encrypted decryption limitation .transferred from the decryption device using the time-varying key to generate the second decryption limitation, and

the contents key generation section generates the contents key based on the second decryption limitation generated by the decryption device.

16. An encryption device according to claim 15, further including

a common key storage section for storing a common key,

a decryption limitation storage section for storing the first decryption limitation,

a first random number generation section for generating a first random number,

a mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device,

a time-varying key generation section for generating the time-varying key using the first random number and the second random number in response to the authentication by the mutual authentication section, and

a second encryption section for encrypting the first decryption limitation using the time-varying key and outputting the second encrypted decryption limitation.

17. An encryption device according to claim 14, further including a decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule in response to the updating of a decryption limitation by the decryption device,

wherein the contents key generation section generates the contents key based on the second decryption limitation obtained by the decryption limitation updating section.

18. An encryption device according to claim 17, further including

a common key storage section for storing a common key,

a decryption limitation storage section for storing the first decryption limitation,

a first random number generation section for generating a first random number,

a mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device,

a time-varying key generation section for generating a time-varying key using the first random number and the second random number in response to the authentication by the mutual authentication section, and

a second encryption section for encrypting the first decryption limitation using the time-varying key and outputting an encrypted decryption limitation.

19. An encryption device according to claim 17, wherein:

the decryption limitation updating section updates the first decryption limitation to the second decryption limitation in advance;

the decryption limitation updating section outputs the second decryption limitation to the contents key generation section;

the contents key generation section generates the contents key from the second decryption limitation; and

the decryption limitation updating section stores the second decryption limitation in the decryption limitation storage section in response to the start of processing by the first encryption section.

20. An encryption device according to claim 16, wherein the

time-varying key generation section generates the time-varying key based on the first and second random numbers and the common key.

21. An encryption device according to claim 16, wherein the contents key generation section generates the contents key based on the second decryption limitation and the time-varying key.

22. An encryption device according to claim 16, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device,

the time-varying key generation section generates the time-varying key based on the first and second random numbers and the data sequence key.

23. An encryption device according to claim 16, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device,

wherein the time-varying key generation section generates the time-varying key based on the first and second random numbers, the common key, and the data sequence key.

24. An encryption device according to claim 16, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device,

wherein the contents key generation section generates the contents key based on the second decryption limitation and the data sequence key.

25. An encryption device according to claim 16, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device,

wherein the contents key generation section generates the contents key based on the second decryption limitation, the time-varying key, and the data sequence key.

26. A decryption device for performing cryptographic communication in association with an encryption device using a contents key, comprising:

a contents key generation section for generating the contents key from a second decryption limitation; and

a first decryption section for decrypting encrypted contents using the contents key generated by the contents key generation section.

27. A decryption device according to claim 26, further including

a decryption limitation updating section for updating a first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and

an encryption section for encrypting the second decryption limitation using a time-varying key, and outputting the first encrypted decryption limitation.

28. A decryption device according to claim 27, further including

a common key storage section for storing the common key,

a random number generation section for generating the second random number, a mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and a first random number,

a time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section, and

a second decryption section for decrypting a first encrypted decryption limitation using the time-varying key.

29. A decryption device according to claim 26, further including a decryption limitation updating section for updating the first decryption limitation to a second decryption limitation in accordance with a decryption limitation updating rule,

wherein a contents key generation section for generating the contents key based on the second decryption limitation updated by the decryption limitation updating section.

30. A decryption device according to claim 29, further including

a second common key storage section for storing the common key,

a second random number generation section for generating the second random number,

a mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and a first random number,

a time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section, and

a second decryption section for decrypting encrypted decryption limitation using the time-varying key.

31. A decryption device according to claim 28, wherein the time-varying key generation section generates the time-varying key based on the first and second random numbers and the common key.

32. A decryption device according to claim 28, wherein the contents key generation section generates the contents key based on the second decryption limitation and the time-varying key.

33. A decryption device according to claim 28, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the decryption device,

wherein the time-varying key generation section generates the time-varying key based on the first and second random numbers and the data sequence key.

34. A decryption device according to claim 28, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the decryption device,

wherein the time-varying key generation section generates the time-varying key based on the first and second random numbers, the common key, and the data sequence key.

35. A decryption device according to claim 28, further including a data sequence key generation section for

generating a data sequence key based on a data sequence input to or output from the decryption device,

wherein the contents key generation section generates the contents key based on the second decryption limitation and the data sequence key.

36. A decryption device according to claim 28, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the decryption device,

wherein the contents key generation section generates the contents key based on the second decryption limitation, the time-varying key, and the data sequence key.

37. A recording medium storing a program for use in causing a computer to perform cryptographic communication with an encryption device using a contents key, wherein:

the program causes the computer to function as:

a contents key generation section for generating the contents key from a second decryption limitation; and

a first decryption section for decrypting encrypted contents using the contents key generated by the contents key generation section.

38. A recording medium according to claim 37, wherein the program causes the computer to further function as:

a decryption limitation updating section for updating a first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule; and

an encryption section for encrypting the second decryption limitation using a time-varying key, and outputting a first encrypted decryption limitation.

39. A recording medium according to claim 38, wherein the program causes the computer to further function as:

a common key storage section for storing the common key;

a random number generation section for generating a second random number;

a mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and a first random number;

a time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section; and

a second decryption section for decrypting a first encrypted decryption limitation using the time-varying key.

40. A recording medium according to claim 37, wherein:

the program causes the computer to further function as a decryption limitation updating section for updating a first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule; and

a contents key generation section for generating the contents key based on the second decryption limitation obtained by the decryption limitation updating section.

41. A recording medium according to claim 40, wherein the program causes the computer to further function as:

a second common key storage section for storing the common key;

a second random number generation section for generating the second random number;

a mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and a first random number;

a time-varying key generation section for generating a time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section; and

a second decryption section for decrypting encrypted decryption limitation using the time-varying key.

42. A recording medium according to claim 39, wherein the time-varying key generation section generates the time-varying key based on the first and second random numbers and the common key.

43. A recording medium according to claim 39, wherein the contents key generation section generates the contents key based on the second decryption limitation and the time-varying key.

44. A recording medium according to claim 39, wherein:

the program causes the computer to further function as a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device; and

the time-varying key generation section generates the time-varying key based on the first and second random numbers and the data sequence key.

45. A recording medium according to claim 39, wherein:

the program causes the computer to further function as a sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device; and

the time-varying key generation section generates the time-varying key based on the first and second random numbers, the common key, and the data sequence key.

46. A recording medium according to claim 39, wherein:

the program causes the computer to further function as a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device; and

the contents key generation section generates the contents key based on the second decryption limitation and the data sequence key.

47. A recording medium according to claim 39, wherein:

the program causes the computer to further function as a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device; and

the contents key generation section generates the contents key based on the second decryption limitation, the time-varying key, and the data sequence key.

ABSTRACT OF THE DISCLOSURE

A copyright protection system comprises an encryption device and a decryption device. Cryptographic communication is performed between the encryption device and the decryption device using a contents key. The encryption device includes a contents storage section for storing contents, a first contents key generation section for generating the contents key based on a second decryption limitation obtained by updating a first decryption limitation, and a first encryption section for encrypting the contents using the contents key and outputting the encrypted contents. The decryption device includes a second contents key generation section for generating the contents key from the second decryption limitation, and a first decryption section for decrypting the encrypted contents using the contents key generated by the second contents key generation section.

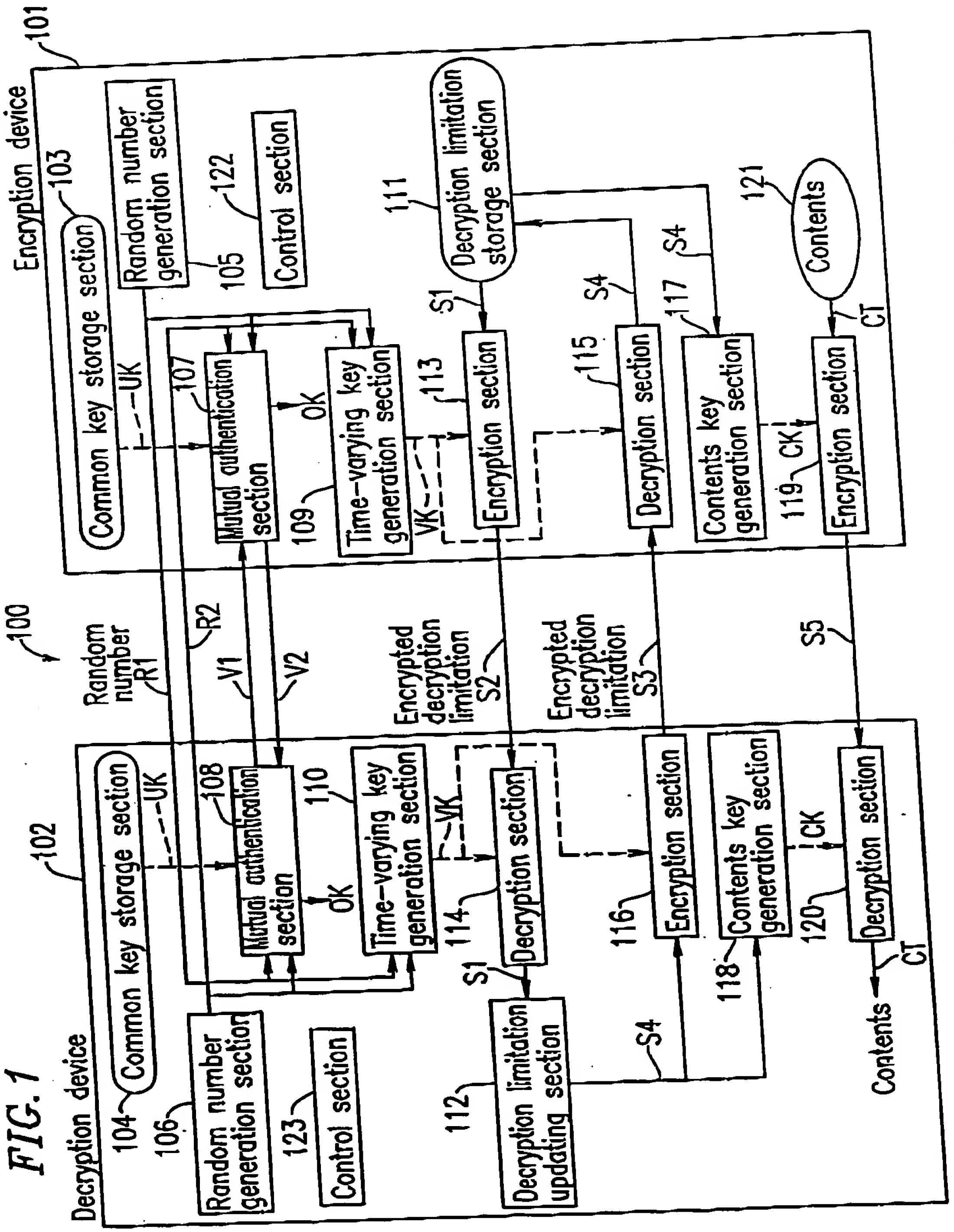
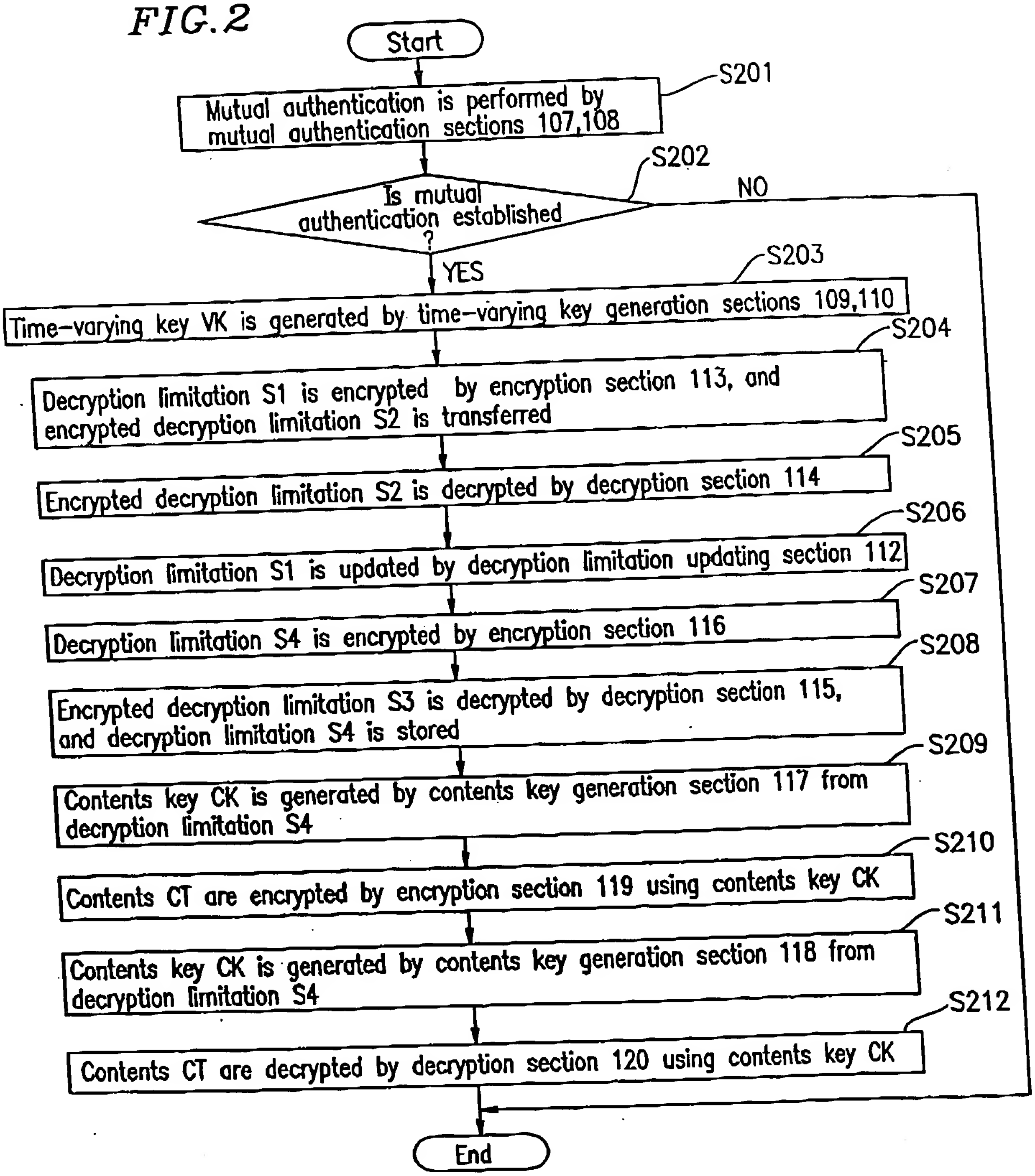

101
Encryption device
103
Common key storage section
UK
Random number generation section
105
122
Control section
107
Mutual authentication section
OK
109
Time-varying key generation section
VK
113
Encryption section
111
Decryption limitation storage section
S1
115
Decryption section
S4
117
S4
Contents key generation section
119
CK
Encryption section
121
Contents
CT
100
Random number R1
R2
V1
V2
Encrypted decryption limitation S2
Encrypted decryption limitation S3
S5
102
Decryption device
104
Common key storage section
UK
108
Mutual authentication section
OK
110
Time-varying key generation section
VK
114
Decryption section
S1
106
Random number generation section
123
Control section
112
Decryption limitation updating section
S4
116
Encryption section
118
Contents key generation section
CK
120
Decryption section
CT
Contents

FIG. 1

FIG.2


Start
S201
Mutual authentication is performed by mutual authentication sections 107,108
S202
Is mutual authentication established ?
NO
YES
S203
Time-varying key VK is generated by time-varying key generation sections 109,110
S204
Decryption limitation S1 is encrypted by encryption section 113, and encrypted decryption limitation S2 is transferred
S205
Encrypted decryption limitation S2 is decrypted by decryption section 114
S206
Decryption limitation S1 is updated by decryption limitation updating section 112
S207
Decryption limitation S4 is encrypted by encryption section 116
S208
Encrypted decryption limitation S3 is decrypted by decryption section 115, and decryption limitation S4 is stored
S209
Contents key CK is generated by contents key generation section 117 from decryption limitation S4
S210
Contents CT are encrypted by encryption section 119 using contents key CK
S211
Contents key CK is generated by contents key generation section 118 from decryption limitation S4
S212
Contents CT are decrypted by decryption section 120 using contents key CK
End

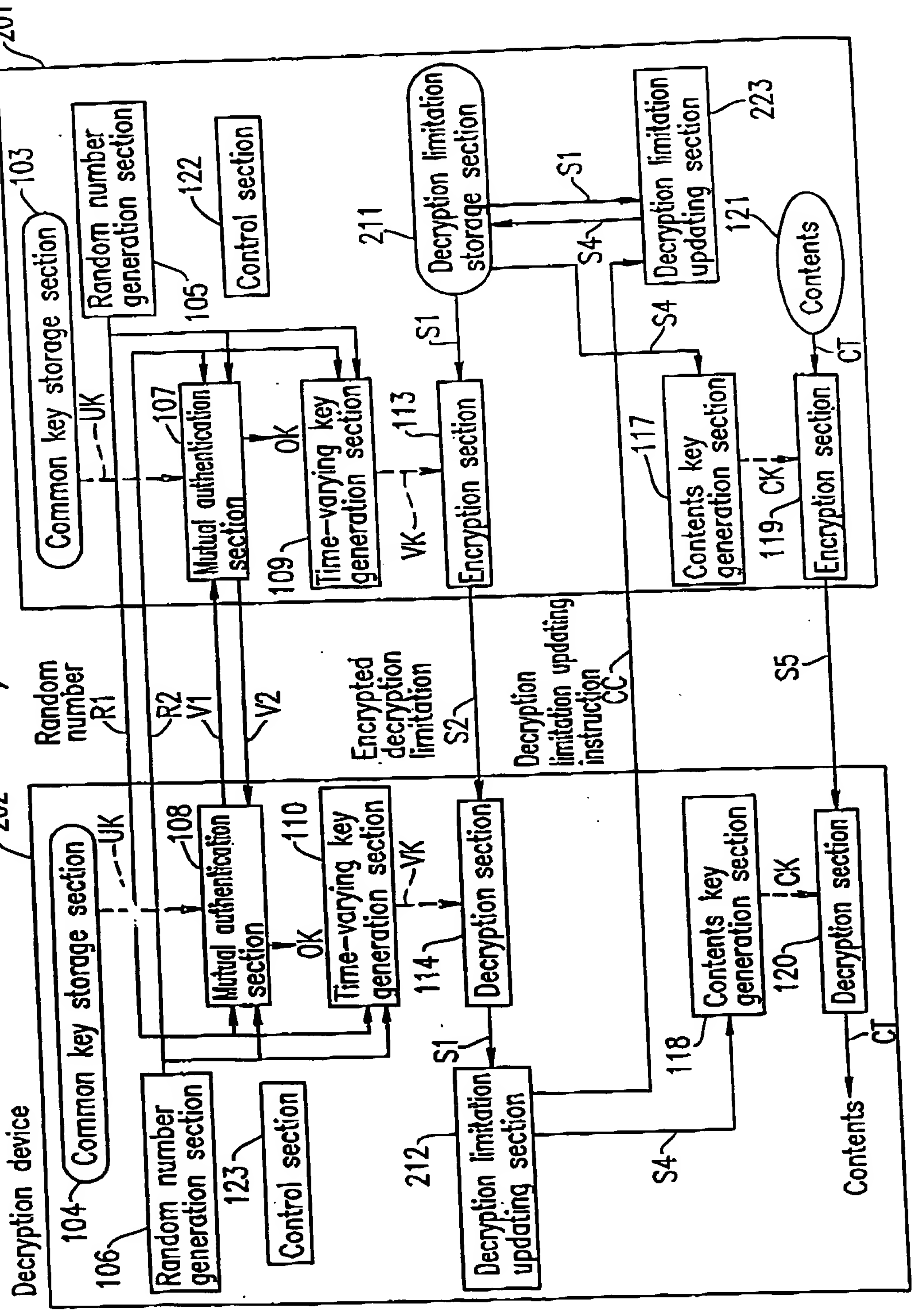

Encryption device
201
Common key storage section
103
UK
Random number generation section
105
Control section
122
Decryption limitation storage section
211
Decryption limitation updating section
223
S1
S4
121
Contents
Mutual authentication section
107
OK
Time-varying key generation section
109
113
VK
Encryption section
S1
S4
Contents key generation section
117
CK
119
Encryption section
CT
200
Random number R1
R2
V1
V2
Encrypted decryption limitation S2
Decryption limitation updating instruction CC
S5
Decryption device
202
Common key storage section
104
UK
Random number generation section
106
Control section
123
Mutual authentication section
108
OK
Time-varying key generation section
110
VK
Decryption section
114
S1
Decryption limitation updating section
212
S4
Contents key generation section
118
CK
Decryption section
120
CT
Contents

FIG.3

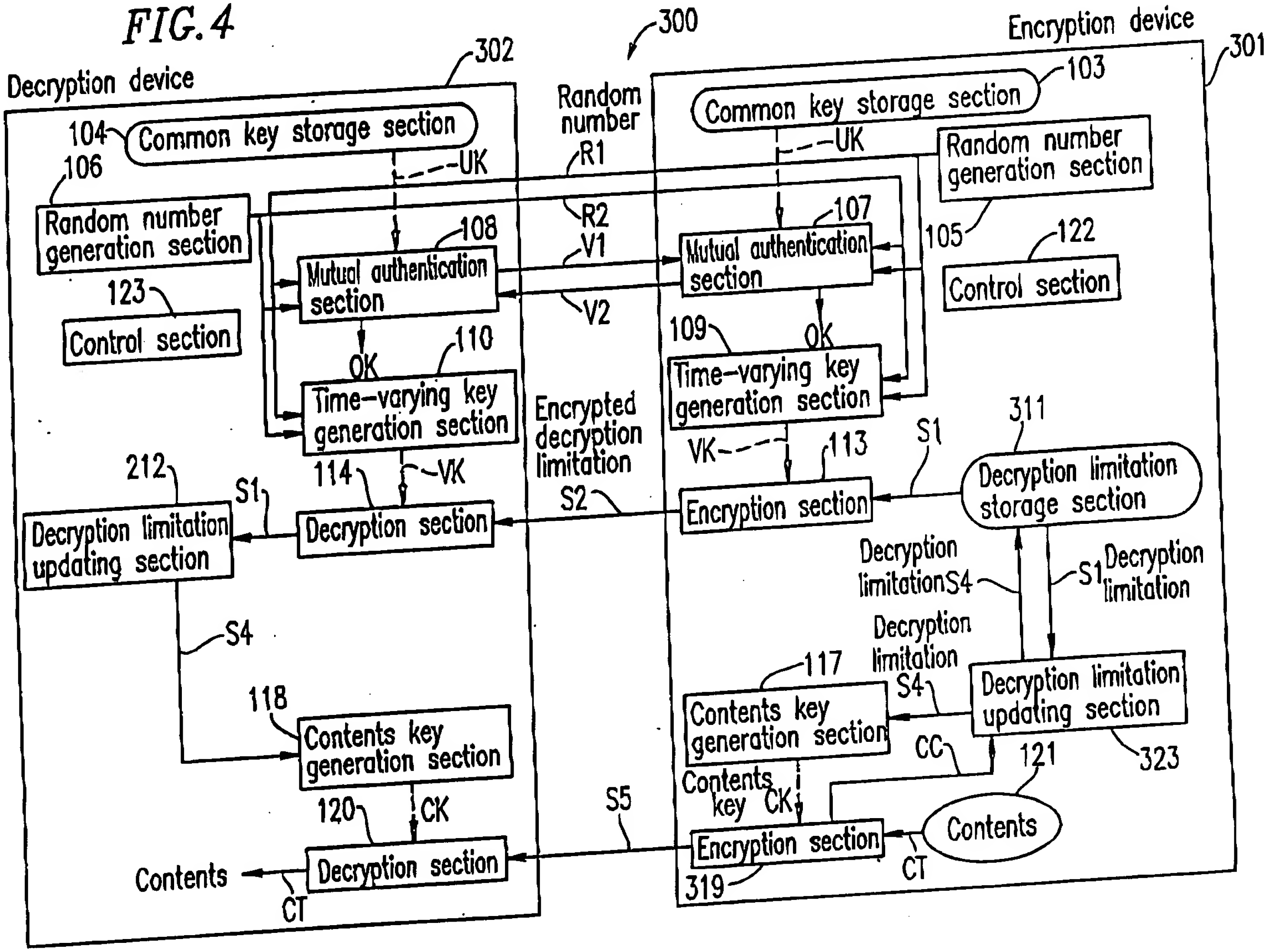

300
Decryption device
302
104
Common key storage section
UK
106
Random number generation section
108
Mutual authentication section
123
Control section
OK
110
Time-varying key generation section
114
VK
212
S1
Decryption limitation updating section
Decryption section
S4
118
Contents key generation section
120
CK
Contents
CT
Decryption section
Random number
R1
R2
V1
V2
Encrypted decryption limitation
S2
S5
Encryption device
301
103
Common key storage section
UK
Random number generation section
105
107
Mutual authentication section
122
Control section
109
OK
Time-varying key generation section
VK
113
Encryption section
S1
311
Decryption limitation storage section
Decryption limitation S4
S1 Decryption limitation
Decryption limitation
S4
117
Contents key generation section
Decryption limitation updating section
323
CC
121
Contents key CK
Encryption section
Contents
CT
319

FIG. 4

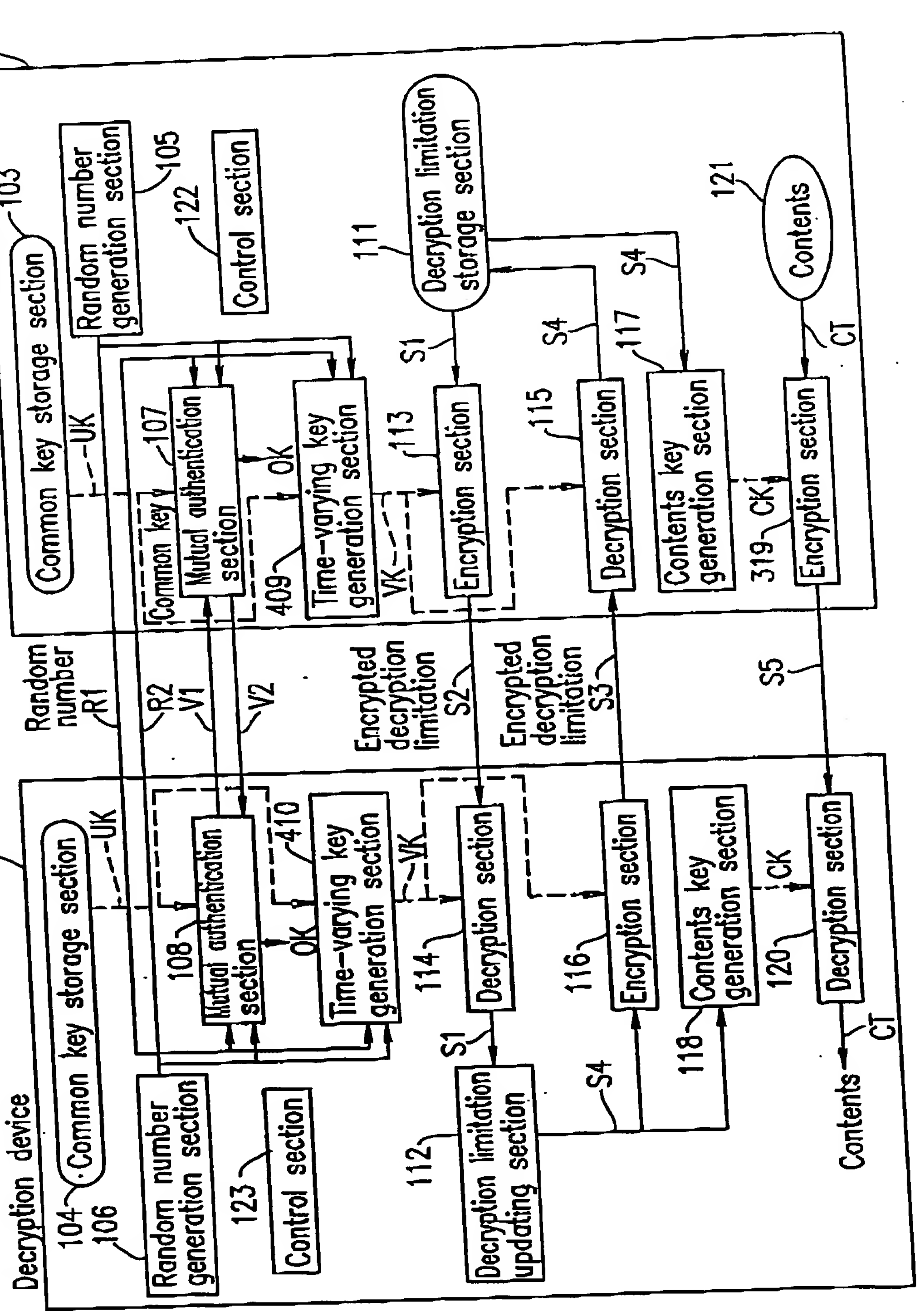
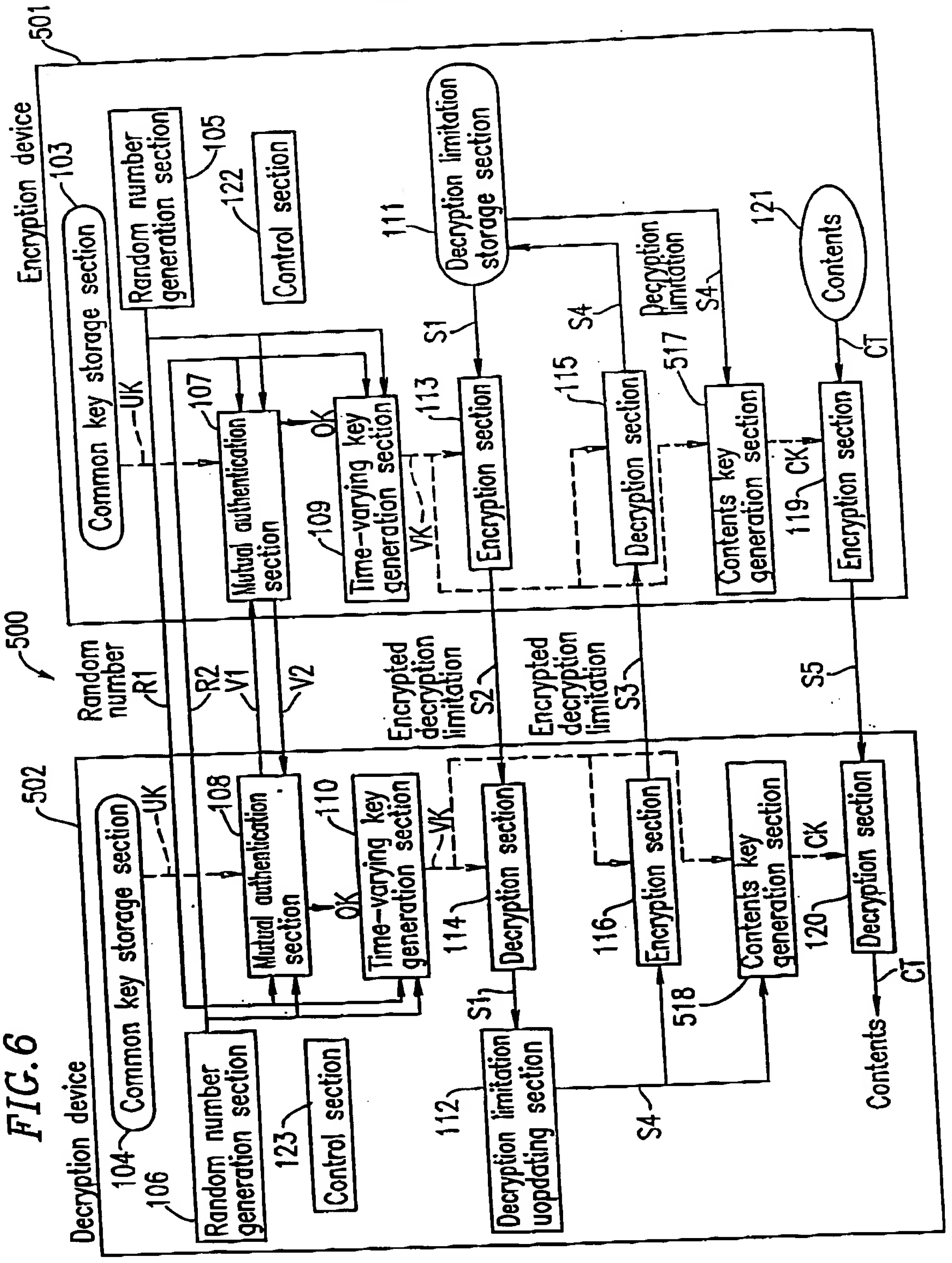

400
401
Encryption device
Common key storage section
103
UK
Random number generation section
105
122
Control section
Common key
Mutual authentication section
107
OK
409
Time-varying key generation section
VK
113
Encryption section
S1
111
Decryption limitation storage section
115
Decryption section
S4
117
Contents key generation section
S4
319
CK
Encryption section
CT
121
Contents
Random number R1
R2
V1
V2
Encrypted decryption limitation S2
Encrypted decryption limitation S3
S5
402
Decryption device
Common key storage section
104
UK
Random number generation section
106
123
Control section
108
Mutual authentication section
410
OK
Time-varying key generation section
VK
114
Decryption section
S1
112
Decryption limitation updating section
S4
116
Encryption section
118
Contents key generation section
CK
120
Decryption section
CT
Contents

FIG. 5



500
501
Encryption device
Common key storage section
103
UK
Random number generation section
105
Control section
122
Decryption limitation storage section
111
Contents
121
Mutual authentication section
107
Time-varying key generation section
109
OK
VK
Encryption section
113
S1
Decryption section
115
S4
Decryption limitation
S4
Contents key generation section
517
CK
119
Encryption section
CT
Random number
R1
R2
V1
V2
Encrypted decryption limitation
S2
Encrypted decryption limitation
S3
S5
502
Decryption device
Common key storage section
104
UK
Random number generation section
106
Control section
123
Mutual authentication section
108
Time-varying key generation section
110
OK
VK
Decryption section
114
S1
Decryption limitation uopdating section
112
Encryption section
116
S4
518
Contents key generation section
CK
120
Decryption section
CT
Contents

FIG. 6

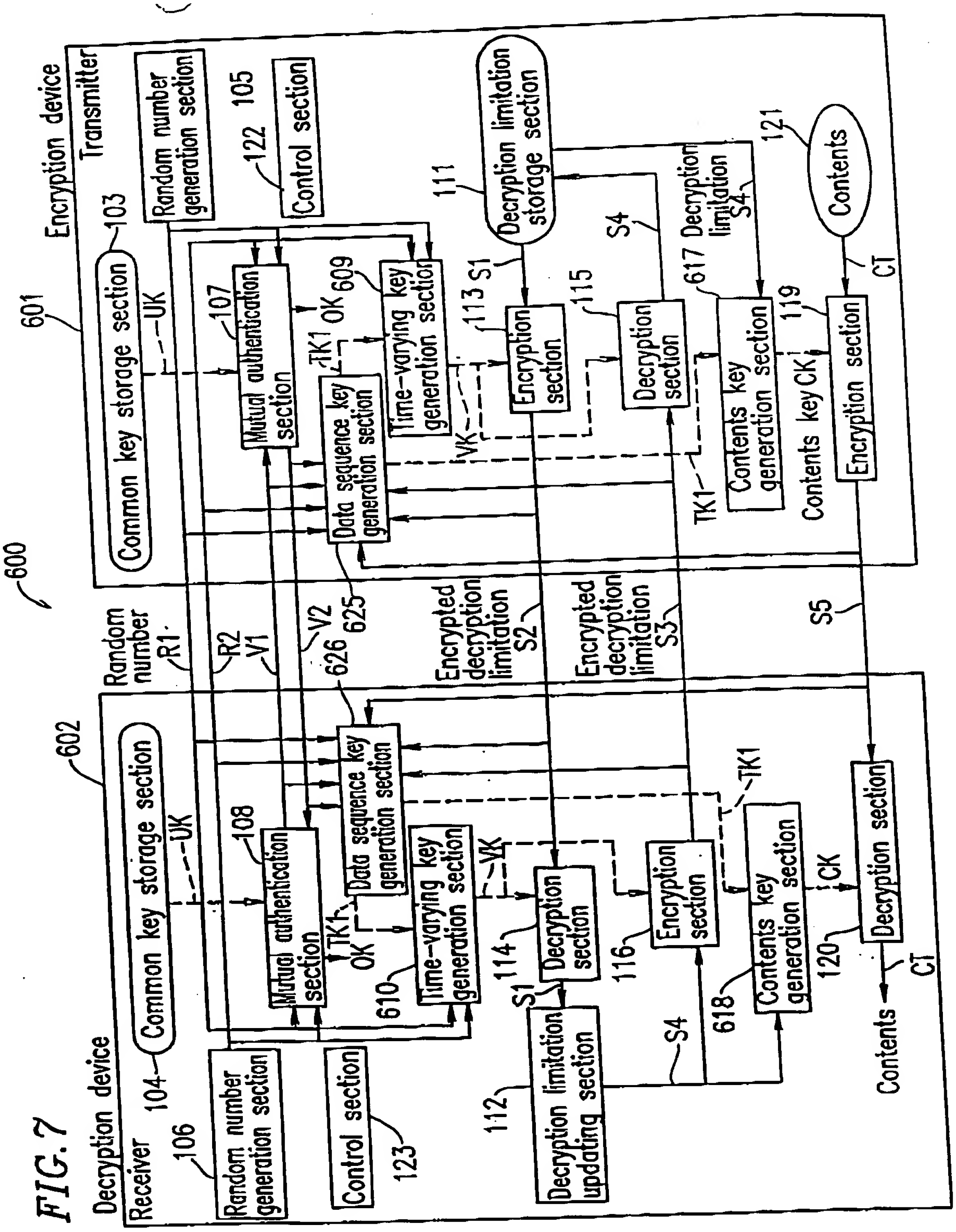

600
601
Encryption device
Transmitter
Common key storage section
103
UK
Random number generation section
122
Control section
105
Mutual authentication section
107
TK1
OK
Time-varying key generation section
609
Data sequence key generation section
625
VK
Decryption limitation storage section
111
S1
113
Encryption section
115
Decryption section
S4
617
Decryption limitation
S4
Contents key generation section
TK1
Contents key CK
119
Encryption section
121
Contents
CT
Random number R1
R2
V1
V2
626
Encrypted decryption limitation S2
Encrypted decryption limitation S3
S5
602
Decryption device
Receiver
Common key storage section
104
UK
108
Mutual authentication section
TK1
OK
Data sequence key generation section
Time-varying key generation section
610
Random number generation section
106
Control section
123
VK
114
Decryption section
S1
Decryption limitation updating section
112
116
Encryption section
S4
618
TK1
Contents key generation section
CK
120
Decryption section
CT
Contents

FIG. 7

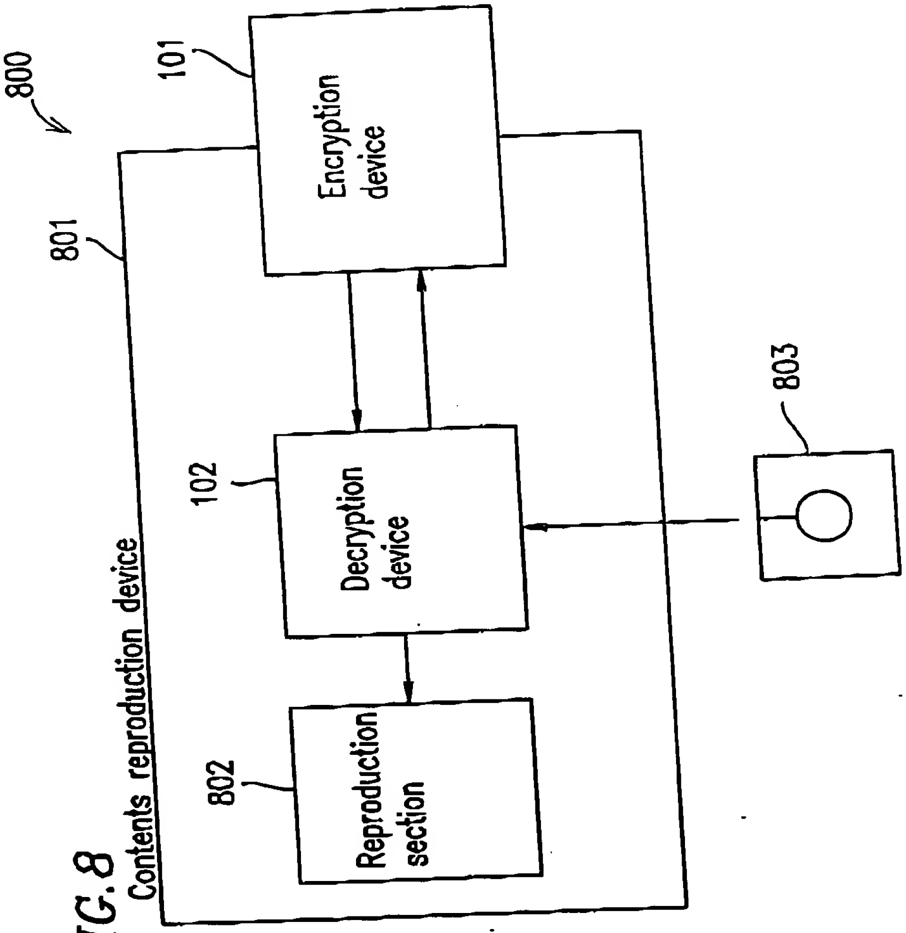

800
801
101
Encryption device
102
Decryption device
802
Reproduction section
Contents reproduction device
803

FIG.8

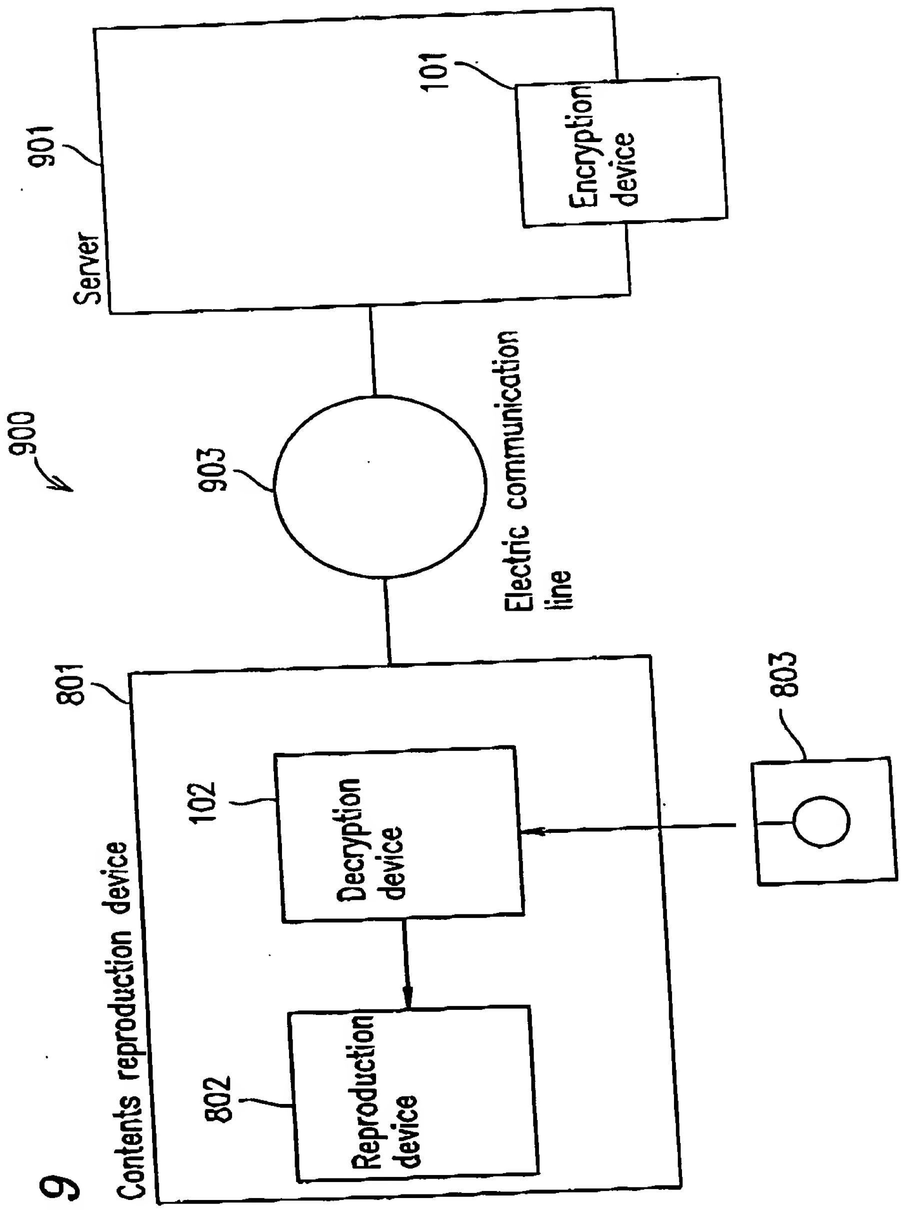

900
Server
901
101
Encryption device
903
Electric communication line
801
Contents reproduction device
102
Decryption device
802
Reproduction device
803

FIG. 9

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年 ４月 ６日

出願番号
Application Number: 特願２０００－１０５５２５

出願人
Applicant (s): 松下電器産業株式会社

２００１年 １月１９日

特許庁長官
Commissioner,
Patent Office 及川耕造

特許庁長官印

出証番号 出証特２０００－３１１２８７

(Translation)

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application : April 6, 2000

Application Number : Patent Appln. No. 2000-105525

Applicant(s) : MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.

Wafer
of the
Patent
Office

January 19, 2001

Kozo OIKAWA

Commissioner,
Patent Office

Seal of
Commissioner
of
the Patent
Office

Appln. Cert. No. Appln. Cert. Pat. 2000-3112877